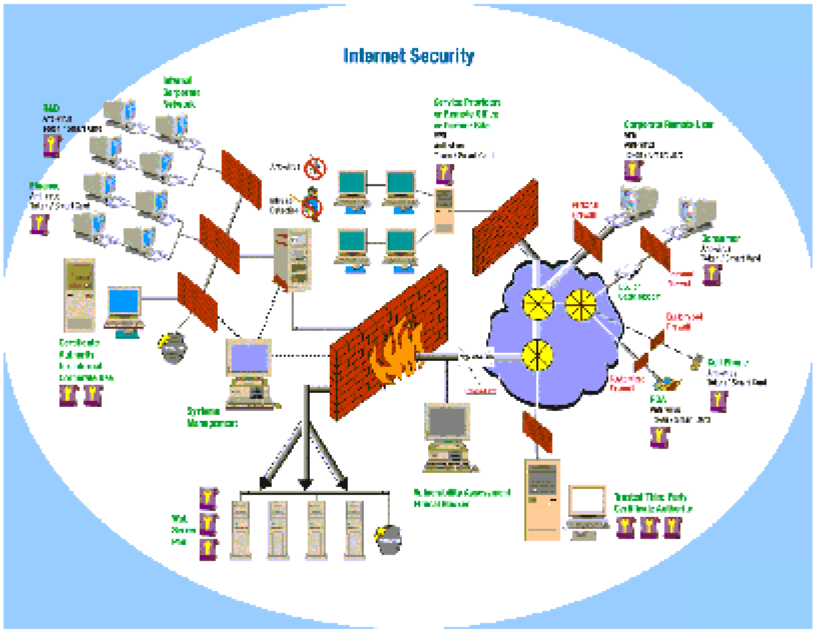
August 2001

UTAH TECHNOLOGY REPORT

INTERNET SECURITY



CRAIG C. BINGHAM
DEREK A. ENGLIS
CHRISTOPHER J. PRESSLER

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The growth of Internet crimes and the increased demand for the digitization of business processes has driven the growth of the Internet security industry. Many government organizations and businesses are racing to secure their information against outside attacks and to update their existing processes to be able to do online transactions. (See **Appendix A** for a diagram of the Internet security industry). As a result, the Internet security industry has developed into a high-growth sector with explosive revenue growth. The Internet security market is divided into four segments: firewall; anti-virus software; authentication, administration, and authorization; and encryption. The firewall and authentication, administration, and authorization, segments have the potential to be the most lucrative.

Utah has the opportunity to establish a regional Internet security, authentication industry within the State. The State of Utah has taken steps to encourage the use and development of Internet security applications, which has caused the growth of promising authentication (PKI) start-ups. These startups have the potential to develop into large successful firms.

The following summarizes our key observations and ensuing recommendations.

OBSERVATIONS

Internet Security Industry

Observation #1: Consolidation is occurring as large players in the industry acquire companies in an effort to offer a wide range of Internet security products. Meanwhile hot new markets continue to develop allowing niche companies to form and continue to build up.

Observation #2: The Internet security market will continue to expand due to the fact that hackers are continually developing new attack techniques. Security vendors, in an effort to stay ahead, are incessantly looking for improved detection and prevention techniques. This should allow room for new technologies or unique implementations to develop and be successful.

Observation #3: In the year 2000, the “Love Bug” infected machines worldwide gaining great press coverage and driving awareness into security issues. This has also occurred more recently with the worm “Code Red.” Although malicious programs and pranks will continue to be a problem, hackers are increasingly turning their attention toward invading corporate information looking for “Data at Rest” (e.g., new product information, credit card numbers, customer lists and employee information). (See **Appendix B** for Glossary of Internet security terms).

Observation #4: Government has played a role in the development of Internet Security through the passage of rules and regulations. Before the recently changed encryption regulations the U.S. government had effectively limited U.S. companies' ability to compete internationally by placing limits on the strength of encryption that could be exported. Alternatively the U.S. government has stimulated demand domestically through regulations especially in the area of encryption technology.

Observation #5: Businesses, in an effort to lower costs, are utilizing the Internet for legally binding transactions and documents. As a result there is an increased demand for Internet security products and services.

Internet Security Industry Leaders

Observation #6: The industry is dominated by a few large companies, although several small niche companies are doing well.

Observation #7: The top Internet security companies are clustered in high-tech regions. Many of these companies are located in California, specifically Silicon Valley, Massachusetts, Washington, Texas, and New York.

Observation #8: Companies in the Internet security industry are relatively new, formed for the most part in the 1990s. This indicates lack of maturity in the product life cycle. The Internet security industry is growing quickly and will remain a vital part of any business using information technology.

Observation #9: There tends to be a large gap in the percentage of market share between the first and second place companies. This indicates that reputation and first movement is gaining importance in this field. A company has to move quickly and reputably to gain a superior brand.

Utah Internet Security Landscape

Observation #10: In recent years the State of Utah has been a leader among states in authentication technology policy and implementation. This has created a seedbed in Utah where authentication technology start-ups have planted themselves.

Observation #11: Within Utah there is a significant presence of Internet security companies including: Access Data Corp, ARCANVS, Inc., Digital Signature Trust, EarthSpeak International, Ingeo Systems, iLumin, Novell, Symantec, and User Trust, Inc.

Observation #12: Utah Internet security companies have special competencies in the authentication segment of the market. These companies include ARCANVS, Inc., Digital Signature Trust, Ingeo Systems, iLumin, and User Trust, Inc.

Observation #13: Utah's Internet security companies are small and privately held. Most are losing money, but have the potential to become large profitable companies.

Observation #14: The State of Utah can facilitate the growth of a regional Internet security technology industry through the continuation of progressive state policy and the expansion of a technology development network that includes business assistance programs, labor force development, research funding, capital creation, and networking forums.

RECOMMENDATIONS

State Government

Recommendation #1: Work to maintain Utah's position as a leading state in the implementation of Internet security policy legislation.

Recommendation #2: Building upon the 2000 Utah Uniform Electronic Transactions Act, which authorizes State agencies to use digital processes for government transactions, the State should work to implement electronic documentation within its separate agencies.

Recommendation #3: Assign a high level State executive as a champion of State Internet security policy and implementation.

Universities

Recommendation #4: Coordinate efforts with State universities to instigate a new Internet security program within the computer science and electrical engineering programs.

Recommendation #5: Work with State universities to build up the Management Information Systems (MIS) programs.

Building Up Utah Internet Securities Companies

Recommendation #6: Facilitate the expansion of Utah's Internet security companies through their pre-IPO growth cycles by helping them obtain second and third round venture capital.

Recommendation #7: Encourage coordinated efforts of State university programs and Utah's Internet security companies by making Internet security a focus of the Centers of Excellence program and creating a non-profit incubator organization.

Recommendation #8: Promote the flow of ideas between Utah's Internet security companies by sponsoring industry forums.

Recommendation #9: Use the Olympics as an opportunity to connect Utah's Internet security companies with potential clients, suppliers, leading Internet security companies, professional business services, and venture capital; ultimately, this will bring together valuable parts of the technology development model.

Focused Recruiting Activities

Recommendation #10: Work to attract encryption companies, including RSA Security, F-Secure, and Symantec.

Recommendation #11: Work to attract a company that develops firewall appliances, such as NetScreen, Nokia, WatchGuard, and SonicWALL.

KEY CONTACTS

Firewall

Companies	Contact	Address	Phone	Website
Check Point (HQ - Israel)	Jerry Ungerman President	3 Lagoon Dr, Ste. 400 Redwood City, CA 94065	650/628-2000	www.checkpoint.com
Cisco	John Chambers President/CEO	170 West Tasman Dr. San Jose, CA 95134	408/526-7208	www.cisco.com
Computer Associates	Sanjay Kumar President/CEO	One Computer Associates Plaza Islandia, NY 11749	631/342-6000	www.cai.com
Microsoft	Steven Ballmer CEO Rick Belluzzo President/COO	One Microsoft Way Redmond, WA 98052	425/882-8080	www.microsoft.com
Network Associates	George Samenuk President/CEO	3965 Freedom Circle Santa Clara, CA 95054	972/308-9960	www.nai.com
Nokia	Sari Baldauf President Nokia Networks	6000 Connection Drive Irving, Texas 75039	972/894-5000	www.nokia.com
Novell	Jack Messman President/CEO	1800 South Novell Place Provo, UT 84606	800/453-1267	www.novell.com
Symantec (Axent Technologies)	John Thompson President/CEO	20330 Stevens Creek Blvd. Cupertino, CA 95014	408/253-9600	www.symantec.com

Antivirus

Companies	Contact	Address	Phone	Website
Network Associates (McAfee)	George Samenuk President/CEO	3965 Freedom Circle Santa Clara, CA 95054	972/308-9960	www.nai.com
Symantec (Norton)	John Thompson President/CEO	20330 Stevens Creek Blvd. Cupertino, CA 95014	408/253-9600	www.symantec.com
Computer Associates	Sanjay Kumar President/CEO	One Computer Associates Plaza Islandia, NY 11749	631/342-6000	www.cai.com
Trend Micro (HQ - Tokyo, Japan)	Mike Conner President, North American Operations	10101 N De Anza Blvd, 2nd Floor Cupertino, CA 95014	408/257-1500	www.antivirus.com

Authentication, Authorization, Administration

Companies	Contact	Address	Phone	Website
Computer Associates	Sanjay Kumar President/CEO	One Computer Associates Plaza Islandia, NY 11749	631/342-6000	www.cai.com
IBM	Samuel Palmisano	New Orchard Rd Armonk, NY 10504	914/499-1900	www.ibm.com
Internet Security Systems	Thomas Noonan President/CEO	6303 Barfield Rd Atlanta, GA 30328	404/236-2600	www.iss.net

RSA Security	Arthur Coviello President/CEO	36 Crosby Dr. Bedford, MA 01730	781/301-5000	www.rsa.com
Entrust	David Thompson Alberto Yepez Co-Presidents/CEO	4975 Preston Park Blvd, Ste 400 Plano, TX 75093	972/943-7300	www.entrust.com
Symantec (Axent Technologies)	John Thompson President/CEO	20330 Stevens Creek Blvd. Cupertino, CA 95014	408/253-9600	www.symantec.com

Encryption

Companies	**Contact**	**Address**	**Phone**	**Website**
RSA Security	Arthur Coviello President/CEO	36 Crosby Dr. Bedford, MA 01730	781/301-5000	www.rsa.com
F-Secure (HQ - Finland)	Christopher Vargas President of US Subsidiary	675 North First St, 5th Floor San Jose, CA 95112 (North America HQ)	408/938-6700	www.fsecure.com
Hitachi America (HQ - Tokyo, Japan)	Yoshihiro Koshimizu	2000 Sierra Point Pkwy Brisbane, CA 94005 (North American HQ)	650/589-8300	www.hitachi.com
Network Associates	George Samenuk President/CEO	3965 Freedom Circle Santa Clara, CA 95054	972/308-9960	www.nai.com
Certicom	Rick Dalmazzi President/CEO	25801 Industrial Blvd Hayward, CA 94545	510/780-5400	www.certicom.com

Other Promising Companies

Companies	**Contact**	**Address**	**Phone**	**Website**
NetScreen	Robert Thomas	350 Oakmead Parkway Sunnyvale, CA 94085	408/730-6000	www.netscreen.com
Palmchip Corporation	Jauher Zaidi Naished Vashi	2595 Junction Ave., 2nd Floor San Jose, CA 95134	408/952-2000	www.palmchip.com
Rainbow Tech., Inc.	Walter W. Straub	50 Technology Drive Irvine, California 92618	949/450-7300	www.rainbow.com
SonicWALL, Inc.	Sreekanth Ravi	1160 Bordeaux Drive Sunnyvale, CA 94089-1209	408/745-9600	www.sonicwall.com
WatchGuard Tech., Inc.	Christopher Slatt James Cady	505 Fifth Avenue South, Suite 500 Seattle, WA 98104	206/521-8340	www.watchguard.com

INTRODUCTION: WHY INTERNET SECURITY?

The Internet connects the world, reducing the cost of communication and doing business. Because of the utility that the Internet offers, the number of consumers and businesses that use the Internet as a tool is growing very rapidly. Internet users are expected to reach over 200 million this year (2001)[1], while "Worldwide net commerce, both business-to-business and business-to-consumer, will hit an estimated $6.8 trillion in 2004."[2] With this increase in Internet use, Internet security is a growing concern.

With the explosion of Internet usage there is also an increase of Internet crimes. According to the FBI nine out of ten companies have reported security breaches since March 1999. A new study by Week Research for PricewaterhouseCoopers, covering 30 countries and nearly 5,000 IT professionals, estimates that hacker attacks will cost the world economy $1.6 trillion in the year 2001.[3]

Part of the 1.6 trillion losses comes from the theft of proprietary information and financial fraud, which have steadily been increasing. In a survey released by the Computer Security Institute and the FBI, 300 businesses were asked what computer crime and abuses had cost their businesses. The following table shows the results of this survey.[4]

Cost of Computer Crime - Total Annual Losses (based on approximately 300 respondents), ($M)

	1997	1998	1999	2000E
Theft of proprietary info	20.0	33.5	42.5	66.7
Financial fraud	24.9	11.2	39.7	56.0
Virus	12.5	7.9	5.3	29.2
Insider abuse of Net access	1.0	3.7	7.6	28.0
Sabotage of data or networks	4.3	2.1	4.4	27.1
Unauthorized insider access	4.0	50.6	3.6	22.6
Laptop theft	6.1	5.3	13.0	10.4
Denial of service	N/A	2.8	3.3	8.2
System penetration by outsider	2.9	1.6	2.9	7.1
Active wiretapping	N/A	0.2	0.0	5.0
Telecom fraud	22.7	17.3	0.8	4.0
Telecom eavesdropping	1.2	0.5	0.8	1.0
Spoofing	0.5	N/A	N/A	N/A
Total Annual Losses:	100.1	136.7	123.8	265.3

Companies are waking up to the fact that their systems need to be more secure and are taking measures to increase security.

> *"…Purchasing security products and setting corporate policies is no longer just for the paranoid. Security has become essential."*
>
> *Cara Cunningham, Red Herring*

The demand for Internet security products is also increasing because of the growing demand for digital transactions that have traditionally been done on paper. Transforming the current paper system to a digital system can reduce the cost of handling business contracts, medical documents, mortgages, loans, notarized documents, and other legal documents. The key to these documents being transformed into digital processes is the augmentation and improvement of digital security. While the benefits are clearly visible the market is not. Internet security companies are in a race to develop products that are both secure and functional, while trying to understand the direction of the market and how to generate revenues.

The growth of Internet crimes and the need for the digitization of business processes has caused the growth of the Internet security industry. The Internet security market is still a high-growth industry and has stayed somewhat healthy in spite of the recent slowdown in the technology sectors.[5] The following is a analysis of the Internet security industry segments, the key Internet security companies, Utah's Internet security landscape, and what steps should be taken to help Utah become a world leader in the Internet security market.

INTERNET SECURITY SEGMENTS

The Internet Security market is composed of four segments:

1. Firewalls
2. Antivirus Software
3. Authentication, Authorization, and Administration
4. Encryption

FIREWALL SOFTWARE MARKET

OVERVIEW

A firewall is a system or group of systems that enforces an access control policy between two networks. How a firewall actually accomplishes its task varies widely, but in principle, the firewall can be thought of as a pair of mechanisms: one that exists to block traffic and the other exists to permit traffic. The type of firewall used will determine whether greater emphasis is placed on blocking traffic or permitting traffic (See **Appendix C**).

Conceptually, there are two types of firewalls:

1. Network layer
2. Application layer

Network layer firewalls generally make their decisions based on the source, destination addresses, and ports in individual IP packets. Modern network layer firewalls now maintain internal information about the state of connections passing through them, the contents of some of the data streams, and so on. One thing that's an important distinction about many network layer firewalls is that they route traffic directly though them, so to use one you either need to have a validly assigned IP address block or use a “private Internet” address block. Network layer firewalls tend to be very fast and tend to be very transparent to users.

Network layer firewalls, also known as firewall appliances, firewalls in a box or fireboxes, are pieces of hardware bundled with software solutions that create a single turnkey system. Fireboxes offer not only basic firewall functionality but also the capacity to incorporate Virtual Private Networks (VPNs), URL filtering, security, policy and bandwidth management.

Application layer firewalls, or software-based firewalls, generally are hosts running proxy servers, permit no traffic directly between networks, and perform elaborate logging and auditing of traffic passing through them. Application layer firewalls tend to provide more detailed audit reports and tend to enforce more conservative security models than network layer firewalls.

Distributed firewalls are another type of software-based firewall. These host-resident security software applications are firewalls place on a multitude of end-user machines and are centrally configured and managed. They are used to protect servers and end-user machines against unwanted intrusion by considering all requests, internal or external, as possible intruders versus traditional firewalls, which consider only external requests as possibly hostile.[6]

Choosing between firewall appliances (hardware) and software-based solutions depends on the needs of the business and offer various advantages. The benefits of each are outlined below.

Hardware

- Appliances offer convenience through an all-in-one approach
- Appliance instillations are less complex
- Appliances are compatible with software solutions
- Appliances have embedded operating systems that are inaccessible to end users, thereby, lowering security threats

Software

- Software-based firewalls are easier to integrate with enterprise-level platforms
- Software-based firewalls offer higher performance scalability
- Software-based versions reduce equipment costs by using companies' already existing hardware

1999 Market Performance

Software

1999 revenue for the firewall software market is $537 million, a 25% growth rate over 1998 revenue of $431 million. There were several factors behind this growth rate, such as:

- The growth of ecommerce among small and medium size businesses
- The increased demand for multiple firewalls to protect end nodes in distributed environments
- The need for upgrades and centralization due to the large growth in Internet usage
- The increased usage of extranets

- The increased adoption of virtual private networks (VPNs) enabling corporations to replace expensive leased lines between corporations and remote offices

Hardware

1999 revenue for the appliance firewall market was $332 million, reflecting an 82% growth rate over 1998. The firewall appliance market can be separated into three segments based on price; high (greater than $10,000); medium ($5,000-$10,000); and low (less than $5,000). Within these segments of the firewall appliance market, revenue from the medium price segment grew the fastest at 175% with the low price segment coming in at second with 152% growth rate.

Worldwide Firewall Appliance Market by Segment, 1998-1999 ($M)

Price Band	1998	1999	1998 Share (%)	1999 Share (%)	1998-1999 Growth (%)
High (>$10,000)	138	216	76	65	56.5
Medium ($5,000-$10,000)	12	33	6	10	175.0
Low (<$5,000)	33	83	18	25	151.5
Total	182	332	100	100.0	82.4

Source: IDC and Salomon Smith Barney

LEADERS

Software

The leaders for the firewall market (software only) are:

1. Check Point
2. Computer Associates
3. Microsoft
4. Network Associates
5. AXENT Technologies (Symantec), Novell

Check Point has been the leader in the firewall software market since 1997. In July of 2001Check Point introduced Check Point Next Generation an open, scalable, centrally manageable and easy to deploy software that enables dramatically reduced communications costs. Check Point Next Generation is being supported by the world's leading hardware platform vendors, including Compaq, IBM, Nokia and Sun Microsystems.[7] Check Point is also in a solid position with its Open Platform for Secure Enterprise Connectivity (OPSEC) Alliance, which develops partnerships with third-party network-management and security vendors.[8]

Computer Associates rose to second place in 1999 achieving 12% market share and $65 million in revenue. In 2000 Computer Associates released eTrust, the complete eBusiness security line package. In April of 2001, the company announced the beta availability of a powerful new eBusiness Infrastructure management solution for Java. Code-named Athena, the solution manages the health and performance of complex, large-scale eBusiness applications based on Enterprise Java Beans (EJB) technology.[9]

Microsoft rose into third place achieving 10% market share on $51.3 million in 1999. In 2000, Microsoft introduced their Internet Security and Acceleration server, an Internet Security and caching server, replacing their Microsoft proxy server.[10]

Network Associates fell from second place into fourth place, with 8% market share and revenues of $41 million. In 1999 Network Associates made a strategic move and established the Security research Alliance with Cisco, Lucent, Sun Microsystems, and the research and development unit of GTE. In 1999, Network Associates' McAfee.com made an IPO.

AXENT Technologies (acquired by Symantec in August of 2000) and Novell were tied for fifth place with revenues and market share of approximately $30 million and 6% respectively. AXENT spurred their revenue in 1999 with the purchase of Compaq's AltaVista's Firewall and AltaVista Tunnel but still had negative growth. Novell's flagship product, NetWare Servers, directory-enabled applications, education and consulting, guided their growth for 1999.

Worldwide Firewall Software Revenue by Vendor (Rank order), 1997-1999 ($M)

					1998-1999
	1997	1998	1999	1999 Share (%)	Growth (%)
Check Point Software Technologies	82.9	140	218.6	40.7	56.1
Computer Associates Int'l. Inc.	8.1	32.1	65.2	12.1	103.1
Microsoft Corporation	7.6	30	51.3	9.6	71.0
Network Associates, Inc.	21	61.9	41	7.6	-33.8
AXENT Technologies	26	33	30.6	5.7	-7.3
Novell, Inc.	10.8	21	29	5.4	38.1
IBM	9.8	17	25	4.7	47.1
Sun Microsystems	5	9.1	14.5	2.7	59.3
Secure Computing Corp.	19	34	8.8	1.6	-74.1
Elron Software	9	8	6	1.1	-25.0
Other	45.7	44.7	46.9	8.7	4.9
Total	244.9	430.8	536.9	100.0	24.6

Source: IDC, 2000

Hardware (Note: The following are leaders for the appliance firewall market for the year 2000. The rest of the report uses 1999 data)

The leaders of the firewall appliance market are separated according to segments in order to better analyze those companies that are poised to be leaders in the future. Those firewalls priced above $10,000 account for the largest portion of sales in the firewall appliance market, with 65% market share. Those priced from $5,000 - $10,000 and less than $5,000 are respectively 10% and 25%.

IDC recently released a report entitled "*Return of the Black Box: Firewall/VPN Security Appliances Unleashed*" in June of 2001. This report segments the firewall/VPN market into five segments based on price. The leaders for these respective segments are:

> $50,000

1. NetScreen
2. Cisco

$10,000-$50,000

1. Cisco
2. Nokia

$5,000-$10,000

1. Cisco
2. Nokia
3. NetScreen

$1,000-$5,000

1. WatchGuard Technologies
2. Nokia Corp.
3. SonicWALL Inc.
4. Cisco Systems Inc.

$300-$1,000

1. SonicWALL
2. NetScreen[11]

Due the large diversity in price the revenue market leader for appliances is different from the shipment market leader. Cisco leads the market for 2000 with 45% market share and SonicWALL lead in shipments with 24% of the market.

Cisco is the market leader in the overall firewall appliance market and holds second place in the overall firewall market. Cisco's products include the PIX firewall, and IOS firewall. Cisco Secure PIX Firewall is the dedicated firewall appliance in Cisco's firewall family and holds the top ranking in market share. A security-specific, value-add option for Cisco IOS Software, the Cisco IOS Firewall enhances existing Cisco IOS security capabilities, such as authentication, encryption, and failover, with state-of-the-art security features, such as stateful, application-based filtering (context-based access control), defense against network attacks, per user authentication and authorization, and real-time alerts.[12]

NetScreen Technologies is a private company based out of Sunnyvale, California. They are currently being funded with venture capital. NetScreen is a company that is playing an increasing role in the firewall market as a newcomer. NetScreen focuses on the higher end firewalls then selling smaller units to these customers to implement as firewalls at remote facilities. Founded in 1997 by individuals from Cisco, Intel and Healtheon, NetScreen started selling their products in 1999 accumulating $8 million in revenue. In the year 2000, NetScreen grew 400% amounting to revenues of $40 million.[13] NetScreen controlled the highest-range market, greater than $50,000, with 57% market share. NetScreen also came in second low-range segment, $300-$1,000, and third in the mid-range segment $5,000-$10,000 (out of five segments).[14]

Nokia Internet Communications, headquartered in Mountain View, California, provides Network Security and Virtual Private Network solutions to ensure the security and reliability of corporate enterprise and managed service provider networks. Nokia partnered with Checkpoint, in 1999, to offer both firewall and VPN-1 capabilities in Nokia's appliances.[15] Nokia gained over 11% market share over the year 2000, demonstrating the fastest growth in the industry. Nokia achieved more than 430% growth in the firewall/VPN security appliance market capturing 21% of the $1,000-$5,000 market share for the total worldwide firewall/VPN appliance market.[16]

WatchGuard Technologies is a pioneer in the creation of the plug-and-play Internet security appliance and server security software. The Company's LiveSecurity Service enables organizations and users to keep their security systems up-to-date, and its ServerLock software provides server content and application security to protect critical data and services against unauthorized or unintentional access or manipulation. Their Firebox System is a scalable firewall and VPN solution for small, mid-sized and large distributed enterprises and data centers. The comprehensive hardware and software solution delivers four key benefits: centralized management, comprehensive security protection (including firewall and Virtual Private Network), the LiveSecurity Service and a choice of plug-and-play Firebox security appliances.[17]

SonicWALL, Inc. is the leading provider of Internet security solutions for broadband customers in the small to medium size enterprise (SME), branch office, telecommuter and education markets. SonicWALL provides firewall security, content filtering, virus protection and VPN capabilities in a single, integrated platform. SonicWALL is in a strong position for addressing high-growth (low-margin) in the firewall market through deals with McAfee for antiviral software and with several integrators and resellers.[18]

GEOGRAPHIC REGION

Software

North America is the largest market accounting for 56% of the revenue generated from software sales. Western Europe came in second with 26%, less than half of the North

American market share. Asia/Pacific region is third with 12%; the rest of the world (ROW) comprises the remaining 7%.

Worldwide Firewall Software Revenue by Vendor Class and Region, 1999 ($M)

	United States	Western Europe	Asia/Pacific	ROW	Total
Vendor Class					
U.S. ISVs	272	114	53	32	470
U.S. SVs	19	14	6	3	42
International ISVs	7	4	4	2	17
International SVs	1	5	2	1	8
Total					
United States	291	129	58	35	512
International	8	8	6	2	24
Worldwide	299	137	64	37	537
Share (%)	55.7	25.5	11.9	6.9	100.0

Source: IDC, 2000

Hardware

In the firewall appliance market North America leads the market with 54% of the revenue. Western Europe comes in second controlling 26% of the market share by revenue.[19]

OPERATING ENVIRONMENT

Software

Windows 32-bit category has taken over Unix's lead in the operating environment with a 42% market share. Unix is in second place with 36%; while in third place are the other host/server environments with 17%. None of the remaining operating environments account for more than 4% of the market, individually (See **Appendix D**).

Hardware

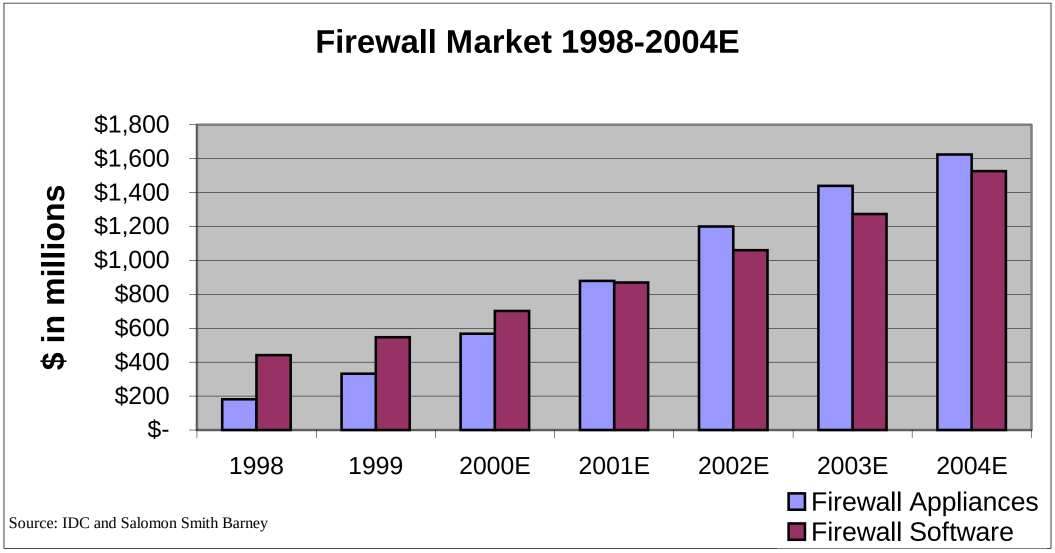
The firewall appliance market is similar to that of the software market with respect to the operating environment.

MARKET OUTLOOK

GROWTH

Hardware and Software

The firewall appliance market is expected to grow faster than the market for software-based firewalls, with a 37% cumulative average growth rate (CAGR) for appliances versus 23% CAGR for software.



Source: IDC and Salomon Smith Barney

Within the firewall appliance market the medium and low price segments are expected to achieve the most rapid growth with 74% CAGR and 54% CAGR respectively. Small to medium sized businesses will be the drivers behind the growth of the firewall appliance market. The low price segment is expected to reach 44% market share in terms of revenue by 2004.

Worldwide Firewall Appliance Market by Segment, 1998-2004E ($M)

Price Band	1998	1999	2000E	2001E	2002E	2003E	2004E	1999-2004E CAGR (%)
High (>$10,000)	138	216	312	352	370	381	381	23
Medium ($5,000-$10,000)	12	33	85	176	297	424	533	74
Low (<$5,000)	33	83	170	352	534	635	711	54
Total	182	332	567	879	1200	1440	1625	37

Source: IDC and Salomon Smith Barney

GEOGRAPHIC REGION

Software

North America will be the largest market in 2004 but is expected to have the lowest CAGR, 12%, out of the four regions represented. Western Europe will remain the second largest market growing at 16%. IDC expects the Asia/Pacific markets to recover boosting revenue with a CAGR of 30%. The ROW revenue is predicted to grow strongly at 29% rate as Latin American companies become more active in ecommerce in 2001 and beyond (See **Appendix D**).

Hardware

North America's lead in the firewall appliance market will decrease from 54% of the revenues to 45% by 2005. During this same period of time it is estimated that Western Europe will increase their share of the market from 26% to 31%.[20]

OPERATING ENVIRONMENT

Software

The leaders by CAGR are as follows:

- Mainframes are forecasted to gain strength as ecommerce servers with firewall capabilities enabled in them become more prevalent, showing a CAGR of 26%. The importance of a high CAGR is lessened with a forecasted market share of only 1% by 2004.

- Platform-independent OSs follow mainframes with a strong CAGR of 25%, but like mainframes are termed insignificant with a forecasted market share of 2%.

- 32-bit Windows is in third place in terms of CAGR with its 23% but unlike the first two it is forecasted to have the highest market share with 53%.

- Unix finishes in fourth place with a 5% CAGR. It is forecasted to lose more market share falling from 36% to 21% by 2004 (See **Appendix D**).

Hardware

Again due to the lack of information we are left to assume that the firewall appliance market, in terms of operating environment, will follow the same model as firewall software.

SATURATION LEVELS

The firewall market still has a positive outlook on growth. At the end of 2000 it was predicted that approximately 50% of the large businesses, 41% of the medium-sized businesses and 14% of small businesses in the United States had firewalls installed. IDC predicts that the market will approach saturation by the year 2004.[21]

MARKET TRENDS

LEADERS

Firewalls are largely recession resistant due to the need of guaranteed security protection in the business environment, but are vulnerable in that customers are looking for more than just a perimeter defense. As such, firewall vendors will continue to evolve into security management companies. Firewall companies will also continue to position firewalls as platforms for a variety of security products, migrating toward an all-in-one solution. Evidence of this is seen in the now norm offering of Firewall/VPN services where firewalls are used in conjunction with Virtual Private Networks, made possible through the use of PKI, to provide a strong source of authentication.

In the software arena there was the rise of the personal firewall market, firewalls less than $100, in the late 1990's as an outgrowth of the distributed firewall market. Personal firewalls differ from distributed firewalls in that they are targeted at home users of always-on, high-speed connections (i.e. cable or DSL modem) and do not offer centralized management. Centralized management gives corporations the ability to update policy management and VPN management easily.

The personal firewall market is expected to eventually disappear, and become a value-added service provided by ISPs, switch vendors, and the distributed firewall market. Most ISPs and switch vendors are expected to make this transition by year-end 2002. In 1999, ISPs made up 5% of firewall software revenue and another 15% of the software revenue through reselling. These numbers are expected to increase to respectively 15% and 40% of software revenue by 2003. Personal firewall vendors in foresight have already begun the transition into distributed firewall vendors. Although revenue from personal firewalls will decline, it will continue to exist after 2003 due to the installed base of old non-firewall based equipment, and through subscription updates (See **Appendix E**).

Distributed firewalls will continue to thrive after the disappearance of the personal firewall market due to the fact that corporations want to maintain control over security of remote access employees and lack of trust for outsourced policy management. As a result, corporations will continue to purchase distributed firewall solutions in order to protect telecommuters, communication networks, and corporate LANs and WANs. Distributed firewalls are also the main component behind the management of firewall services by MSPs and network service providers. These providers are increasingly giving away the software and concentrating on providing service.

FIREWALL SUBMARKET: VIRTUAL PRIVATE NETWORKS

It should be noted that the majority of the information about Virtual Private Networks comes from a document written by Chuck Jones of Salomon Smith Barney.[22]

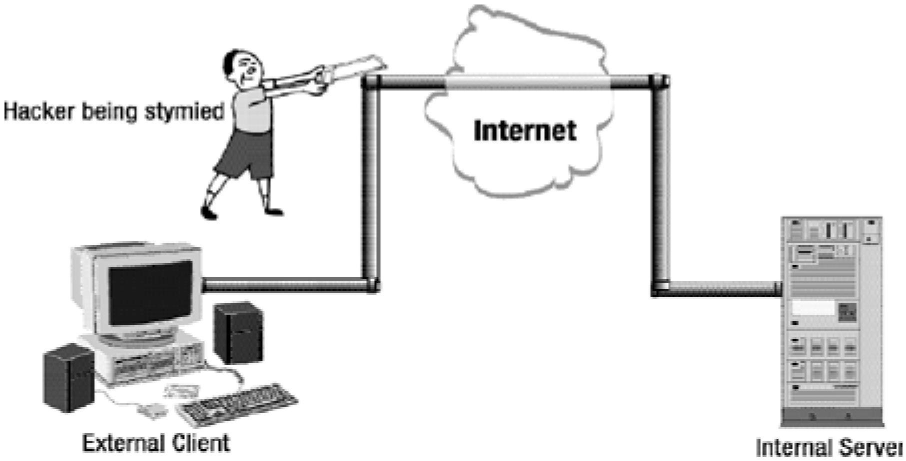
A VPN "is a temporary network connection that creates a secure communications link (or tunnel) between two systems. It combines encryption and communications software with a public network, such as the Internet, to establish a point-to-point connection between two systems in order to transmit data between each other securely."[23] They are included below the firewall market due to their wide adoption in firewalls.

VPN solutions are made up of the combination of three critical technology components; security, traffic control and management.

The security component includes encryption by means of public key infrastructure for the protection of data, authentication to verify identities, and access control to guarantee the users is accessing only those applications they are authorized to use.

Traffic control, the second component, prioritizes traffic in order to deliver reliability, quality of service, and high-speed performance for communications between two systems. This is important to the prevention of bottlenecks congest Internet communications rendering them unsuitable fore critical business applications.

Management is the final critical component of VPN. Management is used to integrate VPNs into the overall security policy. VPNs are also able to provide centralized management from local or remote users and scalability enabling multiple remote users with the ability to access internal networks and applications simultaneously.



Before the arrival of VPNs the primary means of establishing a secure connection were expensive leased lines or frame relay circuits. Typically these methods of establishing secure communications were between two fixed points; this is a major advantage to VPNs due to their scalability (they can be established almost anywhere and are not fixed between two points permanently). Other advantages VPNs are that they are inexpensive compared to the alternatives (because they can be established for as short a period of time as needed) and that they have the ability to easily establish secure communications between telecommuters and the office.

The use of VPNs costs companies approximately 60% less than cost of running other traditional secure methods, and has the added benefit of being able to connect anywhere in the world for as long as need be.

VPN Costs - Per 1,000 Users ($M)

	Traditional Remote Access Server Costs	VPN Costs
Phone/ISP charges	1.08	0.54
User Support	0.3	0*
Capital Expenses	0.1	0.02
T1 Lines	0.02	0.03
Total	1.5	0.59

* Included in user access charges.

Source: Salomon Smith Barney

1999 MARKET PERFORMANCE

1999 revenue for VPNs was $281 million, a 97% growth over 1998’s revenue of $142 million. The growth in this market is attributed to VPNs abilities to offer:

- Cost savings over leased lines
- Flexibility to establish secure transmission lines between different locations temporarily[24]

LEADERS

The leaders for the VPN market are obscure due to the fact that VPN is typically bundled with other products. An example of this is Cisco, which is believed to maintain a significant portion of the enterprise VPN market as a result of their large presence in the firewall and router markets. Check Point is another company that is not listed but would have a significant portion of the market.

With the understanding that those companies that bundle VPN in other products, the leaders in terms of revenue are:

1. Nortel Networks
2. 3Com
3. Intel

Nortel Networks was the leader in the VPN market for 1999 with revenues of $40 million equating to a 14% share of the market. Nortel offers IP VPN Solutions, which enable enterprises to enjoy the reach, accessibility, and flexibility of shared IP networks with the privacy and control of private networks, at a lower cost than private WAN (wide area network) solutions.[25]

3Com came in second for 1999 with revenues of $15 million reflecting a 5% market share. In March of 2000, 3Com unveiled the software, Transcend VPN Client, for its virtual private network switches and routers enabling business-class telephony over VPNs improving client access, security and manageability.[26] 3Com also announced software integration with its Total Control 500 DSL Access Multiplexer product that lets providers sell DSL-based VPN services.[27]

Intel came in third in 1999 with $14 million in revenues and 4% market share. In late 2000, Intel came out with a new VPN broadband router designed specifically for small businesses and branch office users that let them offload processor-intensive VPN and firewall functions from their PCs.[28]

Leaders in the VPN Market (Hardware), 1999 ($M)

	1999	Market Share
Nortel	40	14.2
3Com	15	5.3
Intel	12	4.3
Other	214	76.2
Total	281	100.0

Source: Salomon Smith Barney

MARKET OUTLOOK

Salomon Smith Barney and IDC predict that VPNs will grow at a CAGR of 58% from 1999-2004, ending with $2.8 billion in revenue by 2004. The driving assumption behind this growth is that businesses will continue to adopt the use of VPN as a means of communication as they realize the increased benefits that VPNs offer them such as cost savings, flexibility, and security.

Worldwide Virtual Private Network Market, 1998-2004E ($M)

	1998	1999	2000E	2001E	2002E	2003E	2004E	1999-2004E CAGR (%)
Virtual Private Networks	142	281	463	741	1185	1837	2756	58
Growth		97.9	64.8	60.0	59.9	55.0	50.0	

Source: Salomon Smith Barney

ANTIVIRUS SOFTWARE MARKET

OVERVIEW

Internet Security is a strong industry with a positive outlook. There will always be those (i.e. hackers) who try to render systems inoperable and thus provide a secure future for the Internet Security Industry.

Antivirus software protects against the introduction of malicious programs. Malicious programs come in the form of Trojan Horses, worms, logic bombs, and viruses. Generally when individuals refer to a virus they mean one of these four forms of malicious programs. Each of these programs may have one or more missions, such as theft of data, compromising the integrity or disrupting the service of the user or organization. These malicious codes can be used together or separately in accomplishing their mission(s).

A Trojan Horse is a program that gets its name from Greek Mythology. The program neither replicates or copies itself, but does damage or compromises the security of the computer by disguising itself as an attractive or useful program enticing users to execute it, which by so doing, they damage their system. The program hidden in the Trojan Horse could, for example, be one that causes malicious damage by deleting all of your files on your hard disk, or performing espionage for the attacker by stealing passwords.

A logic bomb is a code that infiltrates your system but does not execute until certain conditions are met. The trigger logic might be a date, a person’s name, a bank account number, or a variety of other conditions.

A worm is a self-contained program that proliferates by replicating itself across a network and may damage many different nodes or compromise the security of the computer through attaching files to outgoing messages.

A virus is code that plants itself in any program it can modify. These forms of malicious content usually come in the form of macros. The Microsoft Concept virus is a typical example of how a virus works. The Microsoft Concept virus infects Microsoft Word causing every document opened by the user to save only as a template file. There are many types of viruses besides the typical virus such as:

- Polymorphic virus: A virus that produces varied (yet fully operational) copies of itself, in the hope that virus scanners will not be able to detect all instances of the virus.

- Stealth virus: A virus that uses any of a variety of techniques to make itself more difficult to detect. A stealth boot virus will typically intercept attempts to view the sector in which it resides, and instead show the viewing program a copy of the sector as it looked prior to infection. An active stealth file virus will typically not reveal any size increase in infected files when you issue the "DIR" command.

Stealth viruses must be "active" or running in order to exhibit their stealth qualities.

Protecting your organization or personal computer from these threats requires antiviral software and cautious behavior. Cautiousness is required because antiviral software typically just protects from known threats.[29]

1999 MARKET PERFORMANCE

Worldwide revenue for the antiviral market reached $1.2 billion in 1999, a 21% growth over 1998. The growth rate from 1997 to 1998 was similar. The antiviral market saw one of their biggest increases from 1996 to 1997 as the antiviral market grew by 118%. The reason for the slower growth is a result of vendors' shifted focus. Vendors have:

- Expanded into security management
- Shifted their focus from the desktop market to servers and gateways
- Switched from a consumer to corporate market
- Moved from a purchase model to a subscription model, selling the right to download updates.

LEADERS

The leaders by revenue for the antivirus software market as of 1999 are:

1. Network Associates Inc. (McAfee Active Virus Defense)
2. Symantec (Norton Antivirus)
3. Computer Associates (Cheyenne InocuLAN)
4. Trend Micro (InterScan)
5. Sophos (Antivirus)

Network Associates Inc. (NAI) leads the market. In 1998, NAI acquired McAfee adding Dr. Solomons to their product line and extending their lead over Symantec. In 1999, NAI had revenue of $470 million resulting in 39% share of the AV market. NAI's revenue growth for the year 1999 was 6% resulting in a loss of market share from the year 1998. NAI is the leader in the corporate market with a 47% market share and in second place in the consumer market with 22% of the market.

Symantec remained in second place for 1999 with revenue of $302 million. This was a 27% increase over 1998 sales and results in a market share of 25%. Symantec was the leader in the consumer market with 41% share and third place in the corporate market with 18% share. The large growth was due to the strong performance of Norton Internet Security and Norton SystmWorks. Symantec's strategic relationship with IBM and Intel should help keep their revenue growth strong. Symantec has taken a partnership stake in Brightmail, a leading provider of solutions for ISPs, ASPs, and portals to control and protect their email systems with integrated antivirus and antispam technology.[30] Symantec acquired AXENT Technologies, a leading provider of products that enable organizations to centrally manage information security, in December of 2000.[31]

Computer Associates (CA) remained in third place with revenue of $162 million in 1999 and 13% market share. CA focused on the corporate market holding second place in that market with 19% market share. Computer Associates announced on May 29, 2001 that they are entering the consumer market again.

Trend Micro was in fourth place with revenue of $120 million and market share of 10% in 1999. Trend Micro concentrated strictly on the sever market and held a commanding lead of the Internet Gateway server space with 58% market share. The company has positioned itself well by developing alliances with Lucent, Cisco, and Compaq. Trend Micro introduced their eDoctor Global Network in the United States in 1999, enabling ISPs, ASPs and MSPs, to deliver transparently maintained, round-the-clock Internet security services to their subscribers. Trend Micro has partnered with a number of the large service providers to provide this value-added service.[32]

Sophos, headquartered in Europe, came in fifth place with revenues of $21.6 million and approximately 2% market share. Sophos had a growth rate of 44% for the year 1999 and is focused on the corporate market. Being a top international provider, Sophos has a positive outlook for continued growth.[33]

Worldwide Antiviral Software Revenue by Vendor (Alphabetical Listing), 1997-1999 ($M)

	1997	1998	1999	1999 Share (%)	1998-1999 Growth (%)
Computer Associates	71.0	122.9	162.0	13.4	31.8
Datawatch	2.1	-	-	0.0	NA
F-Secure	-	11.0	18.8	1.6	70.7
Finjan Software	1.0	2.0	6.0	0.5	200.0
Intel	9.5	-	-	0.0	NA
Network Associates	391.8	445.0	470.0	38.9	5.6
Norman Data Defense	16.7	7.0	12.0	1.0	71.4
Sophos	9.0	15.0	21.6	1.8	44.0
Symantec	160.0	238.0	302.0	25.0	26.9
Touchstone Software	4.8	1.2	-	0.0	-100.0
Trend Micro	61.1	88.8	120.0	9.9	35.1
Subtotal	727.0	930.9	1112.4	92.1	19.5
Other	63.0	66.4	95.6	7.9	44.0
Total	790.0	997.3	1208.0	100.0	21.1

Source: IDC, 2000

GEOGRAPHIC REGION

North America is the largest market accounting for 55% of the revenue generated from antiviral software sales. Western Europe is second with 28%, approximately half that of the North American market share. Asia/Pacific region is third with 11%; the rest of the world (ROW) comprises the remaining 5%.

Worldwide Antiviral Software Revenue by Vendor Class and Region, 1999 ($M)

	United States	Western Europe	Asia/Pacific	ROW	Total
Vendor Class					
U.S. ISVs	596	248	66	51	961
U.S. SVs	6	2	0	0	8
International ISVs	63	86	68	6	223
International SVs	4	6	3	2	15
Total					
United States	602	250	66	51	969
International	67	92	71	8	238
Worldwide	669	342	137	59	1207
Share (%)	55.4	28.3	11.4	4.9	100.0

Source: IDC, 2000

MARKET OUTLOOK

VENDORS

IDC estimates that the worldwide antivirus revenue will increase from $1.2 billion in 1999 to $2.7 billion by 2004. This equates to a compound growth rate of 17%. U.S. vendors currently lead this market controlling 80% of the market. The U.S. is expected to retain approximately the same percentage of market share by 2004 (See **Appendix F**).

OPERATING ENVIRONMENT

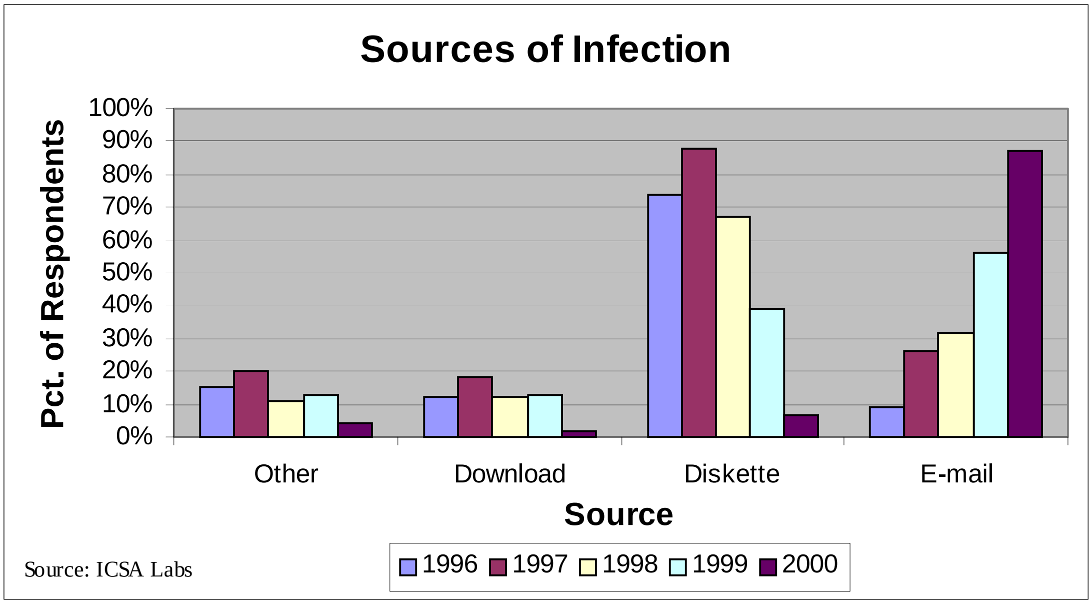
The 32-bit Windows segment and the Mac OS will be the leading growers with a 25% growth rate. IDC estimates that the 32-bit Windows will steal market share from competitors as well as receive migrating market share from the 16-bit Windows environment. By 2004 it is estimated that 32-bit Windows will have 66% of the market share with Mac OS having 5% market share.

GEOGRAPHIC REGION

Revenue from the North American market, the current leader, will grow at 14.5%, but market share percentage will decrease by 6% to approximately 49%. Western Europe is expected to remain second, but its market share will be decreased by 2%, with a 26% market share by 2004. This is largely due to the expected growth in computing environments internationally (See **Appendix G**).

MARKET TRENDS

Corporations have realized that virus protection is a core business requirement as viruses have moved from being an annoyance to a relentless problem. According to ICSA Labs, in 1999 the medium by which the majority of viruses are transmitted has moved from diskettes to email via the Internet.



Source: ICSA Labs

Antivirus protections are migrating to server-based and gateway implementations due to the fact that most viruses are network and/or mail based. NetZero along with other ISPs are now providing protection as a value-added service. Mail gateways are a major growth area because of the Melissa (1999) and the "I Love You" (2000) viruses, which rapidly infected exchange servers. [34] The "I Love You" virus spread worldwide in a matter of hours and alone was estimated to have caused $15 billion in damages. Salomon Smith Barney believes that this figure is the tip of the iceberg due to the fact that most of the costs cannot be quantified by companies and are, therefore, never reported.[35]

Consumers currently pay for antivirus software, but are able to obtain their updates for free. As a result the consumer market for antiviral software is gradually becoming less a part of Internet Security companies' revenue. IDC predicts that antivirus software will migrate from being a separate market to being a value-added feature in other products and services. This is because ISP's are already offering antivirus software as a value-added service with antivirus updates being available for free.

Antivirus vendors are building management consoles, or in other words are entering new markets and expanding their offerings to include other security products. These services are being offered at a single point of contact. This is an important development given that enterprises are demanding these types of services for managing hundreds to thousands of antivirus applications on distributed servers. Some of these technologies are Web filtering/blocking, e-mail scanning, policy management, logging, and reporting for other scanning technologies such as vulnerability assessment, intrusion detection, and firewalls.

To combat the problem of antiviral products being only able to protect against known virus, Antiviral companies are exploring new ways of protecting against malicious or active content. Two of these developments are discussed below.

"Sandboxing" is one of the newest developments in the field of antiviral software. Antivirus products tend to cure known viruses leaving new viruses the ability to penetrate hosts just like their progenitors. "Sandboxing" attempts to prevent the new virus from executing and performing its destructive actions through rules defining what active content can and cannot on the PC. In essence the active content invokes the operating system, but in its attempt to do so the sandbox software intercepts the system call and checks it against a policy database. If the action is allowed by corporate policy then the system call is allowed to proceed, and if the action is not allowed, it is blocked.[36]

Another technology that is already in use by some antiviral software is known as heuristics. Heuristic scanning makes it possible to search for unknown threats by searching for "suspicious" sections of code that are generally found in viral or malicious programs. While heuristics is a promising field, it is not a perfect science and may generate a lot of false alarms or give a false sense of security.[37]

AUTHENTICATION, AUTHORIZATION, AND ADMINISTRATION

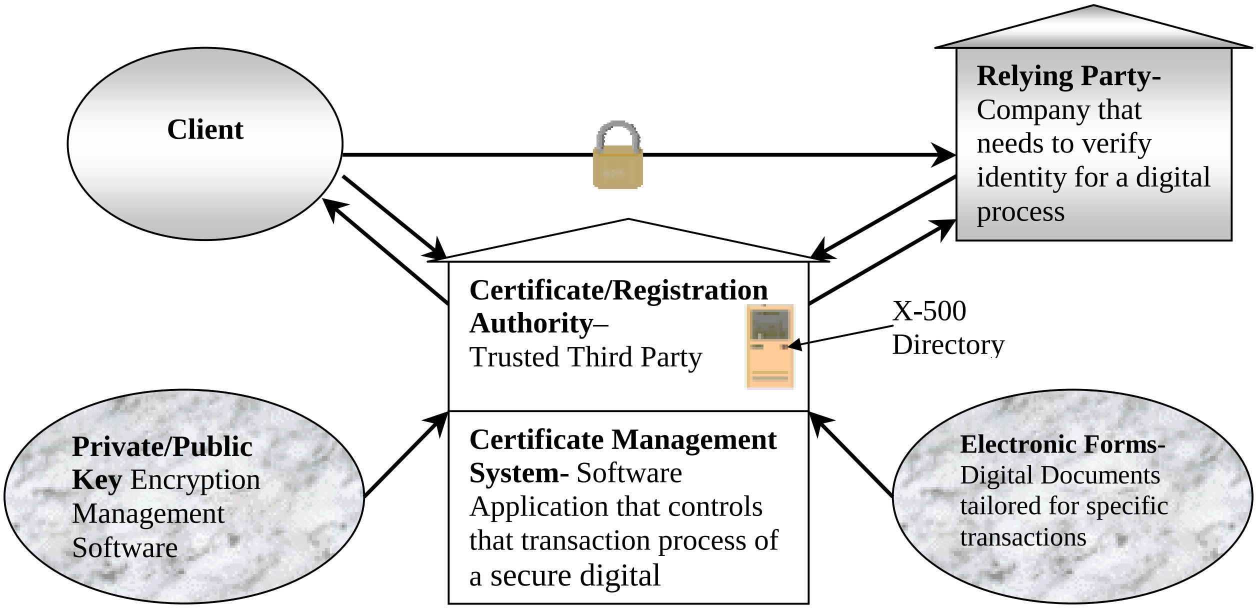
OVERVIEW

AUTHENTICATION: PUBLIC KEY INFRASTRUCTURE

The birth of the Internet and ecommerce has also brought with it an increase in fraud as imposters found it easier to claim to be individuals they were not and with the increase in repudiation, individuals would refuse to pay for merchandise they ordered claiming they did not order it.   Thus arose an increased need to authenticate an individual’s identity.

Digital Signatures are one of the most popular methods for authenticating an individual’s identity. Although digital signatures fall within the authentication segment of the 3A market, the ability to authenticate an individual through digital signatures is reliant upon the encryption technology, public key cryptosystem.

PKI, also called a trust hierarchy, is a merger of encryption technology and processes to form a method of authenticating individuals and therefore is included under the authentication market. While a form of authentication, revenue for the PKI market comes from a mixture of products such as encryption management software, digital signatures, and VPNs, which span across the Firewall, 3A, and encryption Internet security markets. As discussed earlier PKI is a system of digital certificates, CAs, and other RAs that verify and authenticate the validity of each party involved in an Internet transaction. “PKIs are currently evolving and there is no single PKI nor even a single agreed-upon standard for setting up a PKI. However, nearly everyone agrees that reliable PKIs are necessary before electronic commerce can become widespread.”[38]


Client
Relying Party- Company that needs to verify identity for a digital process
Certificate/Registration Authority– Trusted Third Party
X-500 Directory
Private/Public Key Encryption Management Software
Certificate Management System- Software Application that controls that transaction process of a secure digital
Electronic Forms- Digital Documents tailored for specific transactions

Public-key cryptosystems are one component of the public key infrastructure (PKI) and are used to authenticate individuals. Public-key cryptosystems use asymmetric encryption algorithms to create digital signatures that guarantee the authenticity of the signer much the same way a written signature verifies the authenticity of a printed document. Public key cryptosystems do this through employing the use of algorithms, which are used for encrypting data. These asymmetric keys consist of two keys, a public key and a private key, that are mathematically related and can be used for both digitally "signing" a message and encrypting messages in order to keep them private. In asymmetric encryption the owner has both the public key, which is available to anyone who wants it, and the private key, which only the owner has access to. Below is an outline of how asymmetric encryption keys can be used.

- **Public-Key Cryptosystem**
    - *Private (Confidential) Encryption*:
        - **Steps**:
            - Bob creates a message for Alice.
            - Bob procures Alice's public key.
            - Bob encrypts his message using Alice's public key.
            - Bob sends the encrypted message to Alice.
            - Alice decrypts Bob's message using her private key.
        - **Analysis**:
            - **Advantages**: The message is private since no one but Alice can decrypt the message.
            - **Disadvantages**: Alice cannot be sure that Bob is really the sender of the message, since only her key was used to encrypt the message. Indeed, since Alice's public key is accessible to all, anyone could have encrypted the message and then sent it to Alice claiming to be Bob.
    - *Authentication*:
        - **Steps**:
            - Bob creates a message for Alice.
            - Bob encrypts his message using his private key.
            - Bob sends the encrypted message to Alice.
            - Alice procures Bob's public key.
            - Alice decrypts Bob's message using Bob's public key.
        - **Analysis**:
            - **Advantages**: Alice knows the message came from Bob. That is, the message is authenticated, since no one else but Bob could have encrypted the message with Bob's private key. Forgery of Bob's signature is infeasible (but not impossible), so that a presumption arises that Bob signed the message.
            - **Disadvantages**: There is no assurance of privacy. All that is needed to decrypt the message is Bob's public key. Since Bob's key is public, anyone in possession of the message can decrypt the message.

- *Combination: Private Encryption/Authentication:*
    - **Steps**:
        - Bob creates a message for Alice.
        - Bob authenticates the message by encrypting it with his private key.
        - Bob procures Alice's public key.
        - Bob secures the message by encrypting it with Alice’s public key.
        - Bob sends the message to Alice.
        - Alice decrypts the message with her private key.
        - Alice procures Bob’s public key.
        - Alice reveals and authenticates the message by decrypting it with Bob’s public key.
    - **Analysis**:
        - **Advantages**: The message is both private and authenticated.
        - **Disadvantages**: Both Alice and Bob must have ready access to the other's public keys and must be sure that each key belongs or is “bound” to the other. [39]

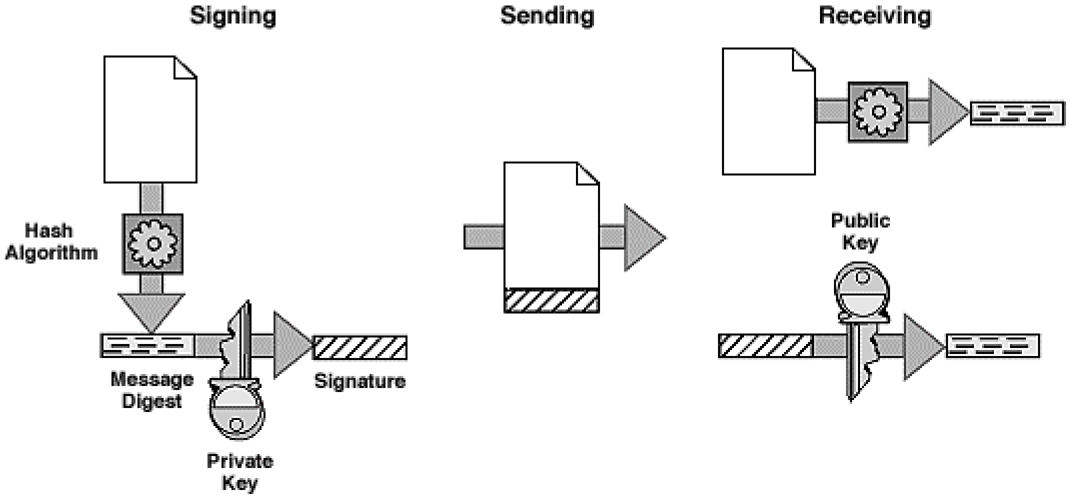
PKI is an important part of Internet security and is gaining in importance, as the Internet is increasingly being used for transactions. Public key cryptosystems are the mortar that holds together the PKI that makes the process of using digital signatures work. [40] Other fundamental components of PKI include a network of certificate management systems (CMSs) used to manage certificates lifecycles; X.500 directories used for storing public encryption keys, public information about certificate subscribers and verifying digital certificates; registration authorities (RA) to verify that individuals are who they say they are; certification authorities (CA) to manage the PKI and CMSs; and forms to provide digital documentation for specific legal transactions.[41]

Most registration authorities are also certification authorities that work in conjunction with certification authorities for the issuance of digital signatures. CAs are trusted third party vendors, who currently make their money by charging individuals or organizations for issuance of private and public keys and by charging relying parties (i.e. merchants, individuals, etc…) for the number of requests they make for public keys to verify digital signatures. Among the CAs there are different niches that they are trying to occupy depending upon their view of what will be the market outcome.

The strength of validity that a digital signature has depends upon the authentication process used by the registration authority to validate the individual who was issued the digital signature keys. Although there are differences in the validity strength of digital signatures there appears to be a migration toward common ground. The validity of a digital signature is also based upon whether or not the integrity of the private key has been compromised through theft, a virus, or a rogue program.

Symmetric key encryption is another method of encrypting communication of data. This method is not used for the authentication of individuals but in encrypting data and as such will be discussed in greater detail in the encryption market.

If the information sent needs additional verification or increased security it may have a hash algorithm ran on it. A hash algorithm is a one-way algorithm that calculates a "hash" value that is unique to the message and is used as an additional layer of security to verify that the message was not altered. "One way" means it's easy to input A and get B, but it's impossible--or nearly impossible--to work backward from B to A. An individual wanting to send a secure message that also verified that it remained unaltered during transmission would first type the message they wished to send and then run it through a hash algorithm. The hash result would then be attached to the message and sent to the recipient. Following the verification of the sender, the recipient would then run the same hash algorithm on the message. If the hash algorithm ran by the recipient, produces the same result as the sender's, the recipient can safely assume that the message was unaltered during transmission.[42]



When the sender signs the document, it is passed through a hashing algorithm to create a message digest and encrypted using the sender's private key.

The signed message is sent across the network.

When the recipient verifies the sender's signature, the same hashing algorithm is used to create a message digest and the signature is decrypted using the sender's public key. If the two are identical, the signature is valid and the document has not changed since it was signed.

Source: Verisign, Inc.

Lawmakers are one of the components driving this industry though the passage of laws making digital signatures valid in a court of law. The following are some of the key laws signed with respect to digital signatures

- Electronic Signatures in Global and National Commerce act or E-sign is a federal law, signed by President Clinton on June 30, 2000, that allows digital signatures to be recognized legally starting October 1, 2000.[43]

- Uniform Electronic Transactions Act (UETA) is a uniform law designed to remove barriers to electronic commerce by validating and effectuating electronic records and signatures. To the extent that a State has a Digital Signature Law, the UETA is designed to support and compliment that statute.[44]

AUTHORIZATION

Authorization is the process by which a particular authenticated individual is identified as authorized to access a particular service or datum. This concept is often expressed as a question (i.e., Can this user do what they are asking to do?) whether the request is to access information, modify information, or take a specific action.[45] It should be noted that strong authentication mechanisms play a part in supporting strong authorization mechanisms.[46]

One of the better-known authorization mechanisms is single sign-on (SSO). Through SSO companies configure users with the ability to enter their password and user ID once to gain access to all authorized functions. It also enables central management the ability to manage accounts with ease. It helps with security by allowing the user to remember the password rather than writing it down. By the same token it also offers increased security threats. A hacker only has to crack one password to gain access to all that the user is authorized to use.[47]

ADMINISTRATION

Administration offers companies the ability to administer policy in areas such as web use and email use. Through administration of these functions companies are able to increase the productivity of workers and reduce bandwidth consumption by limiting what employees can use these resources to do.

Companies want software that offers them the ability to manage a broad rang of products such as intrusion detection, email scanning and web filtering. The ability to administer these functions increases productivity. Intrusion detection reduces the severity of Internet attacks resulting in increased network and host uptime and frees up IT personnel to work on application development. Through Web filtering companies with limited bandwidth can eliminate employee distractions. Email scanning enables companies to ensure that intellectual property is not compromised, reduce distractions, and protect against litigation by employees misguided attempts at sexually or racially oriented humor.

1999 MARKET PERFORMANCE

The 3A software market consists of many applications including security management, single sign-on, intrusion detection and public key infrastructure/certificate authority.

Worldwide revenue for the 3A software market climbed to $2.1 billion in 1999, a 41% growth over 1998. The major driver for this growth was the advent of the Internet, ecommerce, and remote access (See **Appendix H**).

LEADERS

As a reflection of the strength in the mainframe and Unix operating environments, the top two leaders in the 3A software market, Computer Associates and IBM, outpaced the other major vendors by a wide margin. The top leaders in terms of revenue are:

1. Computer Associates
2. IBM
3. Internet Security Systems
4. RSA Security
5. Entrust Technologies
6. AXENT Technologies

Computer Associates (CA) was the 1999 market leader and shows no signs of letting down. In 1999 CA had revenue of $502 million reflecting a market share of 24%. CA focuses primarily on security management, authorization, and authentication. They utilize Unicenter TNG product as the central hub for all of their security products.

IBM holds their spot as the number two vendor in 1999 with revenue of $290 million, reflecting a market share of 14%. The major portion of revenue generated by IBM comes from their focus on the mainframe, S/390, and Unix security management products. IBM's growth rate for 1999 was approximately 35%.

Internet Security Systems (ISS) rose third place with $77.7 million in revenue equating to a 3.7% market share. In 1999, ISS acquired Netrex Secure Solutions in it bid to migrate from a software provider to a managed-security solution (MSS) company. As an MSS, ISS will manage a client's security service for a monthly fee, giving ISS a more predictable revenue stream. According to IDC, MSS will be fastest growing segment in the Internet security industry.

RSA Security, Entrust Technologies, and AXENT tie for fourth place with around $72 million in revenue equaling approximately 3.5% market share (See **Appendix H** for a complete list of companies).

GEOGRAPHIC REGION

Similar to the other segments of Internet Security, North America holds a commanding lead with 58% of worldwide revenue. Europe generates 26% of the market revenue followed by Asia/Pacific at 11%. ROW is the remaining 5% (See **Appendix I**).

OPERATING ENVIRONMENT

Most 3A products are oriented toward servers. As a result, market leadership belonged to Unix with $759 million in revenue yielding 36% market share in 1999. 32-bit Windows was in second place with revenue of $578 million and 28% of the market. Coming in third place was mainframe (S/390) environments. Mainframes accounted for $451 million resulting in 22% market share. None of the remaining operating environments accounted for market share greater than 4% (See **Appendix J**).

MARKET OUTLOOK

Revenue growth for the 3A market is forecasted to grow at a 28% CAGR over the years 1999 to 2004. If consistent with the forecasted growth rate revenue will increase from $2.1 billion in 1999 to $7.1 billion by 2004 (See **Appendix I**).

GEOGRAPHIC REGION

IDC forecasts that although the 3A market is growing at 26% CAGR, North America will lose 3% of their market share of worldwide revenues by 2004 owing a commanding lead still at 55% of revenues. Western Europe is expected to increase slightly to 27% with a CAGR of 29%. The ROW market will grow the fastest with a 32% CAGR, followed by Asia/Pacific at 31% CAGR (See **Appendix I**).

OPERATING ENVIRONMENT

IDC predicts that although Unix will retain the greater share by 2004 growing at a CAGR of 17% it will lose market share falling from 36% to 24%.

32-bit Windows is expected to gain on the Unix operating environment although the majority of security deployments will remain on Unix systems. IDC forecasts the 32-bit Windows operating environment growing at a CAGR of 30%, increasing their market share from 28% in 1999 to 30% by 2004.

IDC predicts that due to the importance in very high-end ecommerce sites, mainframes will grow at a CAGR of 19%. Although there is significant growth in mainframes they are expected to lose market share dropping from 22% in 1999 to 15% by 2004 (See **Appendix I**).

VENDORS

U.S. vendors controlled the market in 1999 with a commanding 84% of the worldwide market, compared to international firms' 16% share. The U.S. is expected to be challenged in retaining this large of the percentage of the market as new international competitors enter the market, especially from Postal Telegraph & Telephony (PTT) organizations in Europe and Asia/Pacific in the PKI/CA submarket, but consolidation among U.S. vendors will maintain the same market share percentages into 2004 (See **Appendix J**).

MARKET TRENDS

AUTHENTICATION

Strong authentication will become increasingly important for establishing secure transactions and communications. Authentication has become and will continue to become more important to businesses due to the fact that establishment of identities lowers fraud costs, lowers credit card rates, and reduces the repudiation rate. PKI and other authentication products offered by vendors such as Arcot, RSA and Vasco are critical elements that are the foundation of the authentication market. New niches within the authentication segment will continue to develop and offer users the ability to reduce paper handling and sign and/or access documents that previously required a physical presence.

Wireless devices, such as cell phones and personal digital assistants (PDAs) are being used more and more to do online transactions. This has created demand for Internet security products that protect wireless communication devices. Thus, the market for Internet security products will continue to grow for new devices as well as for existing products.[48]

AUTHORIZATION

Web-based authorizations and SSO models will continue to merge enabling the users with deeper and broader application access, increasing transactions. With an increase in transactions and a decrease in human interactions costs should decrease.

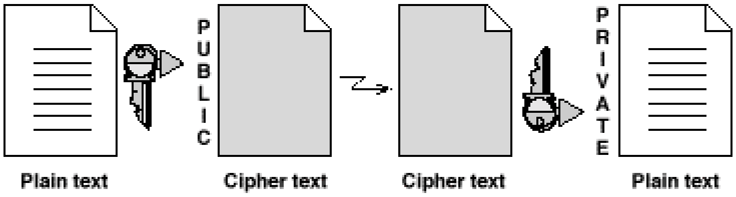
ADMINISTRATION

IDC predicts that as the MSP and ASP models are increasingly implemented, self-administration could mean a huge cost saving and become a powerful element in scaling these environments into millions of customers.

ENCRYPTION

OVERVIEW

Encryption is a method of converting data from an understandable form called plain text into an incomprehensible form known as cipher text via an algorithm. Decryption is the process of converting encrypted data back into its original form, making in it legible.



Source: SET Business Description

Encryption has been around for almost as long as the ability to communicate. Julius Caesar used encryption, in a simple form, for messages containing sensitive data. Simple ciphers include such things as rotation of letters in the alphabet, and substituting letters for numbers. Complex ciphers work by sophisticated mathematical algorithms that rearrange the data into digital signals. Sometimes cipher text is incorrectly referred to as a “code”, which is a means of communicating a signal without the intent of keeping it a secret (e.g., Morse code and ASCII).[49]

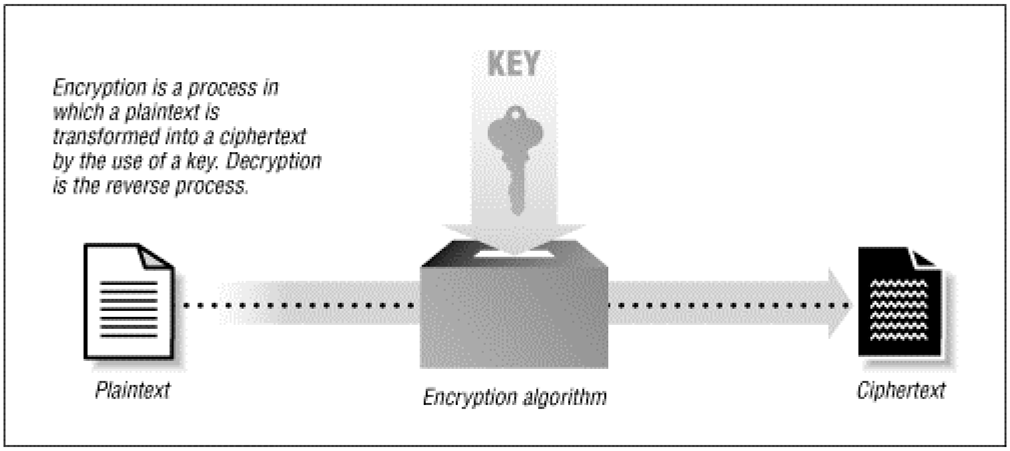
The ability to decrypt a message is dependent upon having the right key. The key is an algorithm that “undoes” the work of the encryption algorithm. Alternatively computers can be used in an attempt to “break” the key. This is usually a time consuming process as the time required to “break” a key becomes increasingly difficult as the bits used in encrypting the message increase, which in turn exponentially increases the strength of the encryption (See **Appendix K**).

Wireless communications have an especially important need for encryption/decryption because wireless circuits are easier to "tap" than their hard-wired counterparts. Nevertheless, encryption/decryption is a good idea when carrying out any kind of sensitive transaction, such as a credit-card purchase online, or the discussion of a company secret between different departments in the organization. The stronger the cipher -- that is, the harder it is for unauthorized people to break it -- the better, in general. However, as the strength of encryption/decryption increases, so does the cost and time required in decrypting the message even with the key.[50]

There are two methods of encrypting data: asymmetric encryption and symmetric encryption. Asymmetric encryption was covered in the authentication market as a result of its use in authenticating parties. Symmetric keys utilize the same private key to both encrypt and decrypt messages. Only the two parties involved in sending the messages have the key. This method tends to be a relatively quick method of encrypting and decrypting messages and offers ease of use.

- **Private Key Cryptosystem:**
    - **Steps**:
        - Bob creates a message for Alice.
        - Bob encrypts the message using a private key known to both Alice and him.
        - Alice decrypts the message using Bob's and her private key.
    - **Analysis**:
        - **Advantages**: This method assures privacy and is faster than any other method of encrypting/decrypting.
        - **Disadvantages**: This method does not offer the ability to authenticate an individual. This method would not be manageable on a large scale due to the number of keys that would be required. For example, 10 people will need 45 keys and 100 people would require 4950 keys. This would also lead to compromised security, as individuals write passwords down in order to remember them.[51]

Advanced Encryption Standard (AES) will be a new Federal Information Processing Standard (FIPS) that should be completed by the end of this summer. The AES is a cryptographic algorithm that will be used by U.S. Government organizations (non-military) to protect sensitive but unclassified information. The military will still retain use of their Triple DES. The National Institute of Standards and Technology (NIST) will submit the final proposal for AES to the Secretary of Commerce after review of public comments, which ended on May 29, 2001.[52] NIST anticipates that the AES will be widely used on a voluntary basis by organizations, institutions, and individuals outside of the U.S. Government - and outside of the United States - in some cases. Two Belgium researchers, Dr. Joan Daemen and Dr. Vincent Rijmen, developed the algorithm that is to be used as the standard.[53]


Encryption is a process in which a plaintext is transformed into a ciphertext by the use of a key. Decryption is the reverse process.
KEY
Plaintext
Encryption algorithm
Ciphertext

Source: SET Business Description

1999 Market Performance

The encryption market's worldwide revenue for 1999 was $134 million, a growth of approximately 33% over 1998's level. This revenue figure includes revenue from the first layer of development tools and algorithms, and revenue from discrete applications that provide file encryption services. There may be a small amount of double counting in this figure given that software developers license algorithms and/or toolkits in the development of their applications. IDC when determining this figure deemed it to be small and as such statistically insignificant.

Leaders

The leading vendors in the 1999 encryption market are

1. RSA Security
2. F-Secure
3. Hitachi
4. Network Associates
5. Certicom

RSA Security led the encryption market in 1999 with revenues reaching $51.2 million and a market share of 38%. The nearest competitor had approximately ¼ of the revenue of RSA.

F-Secure achieved $12.5 million in revenue with approximately 9% market share in 1999.

Hitachi was right behind F-Secure in terms of revenue and market share, with approximately $11.4 million in revenue and 9% market share.

Network Associates and Certicom were tied for fourth with approximately $7 million in revenue and 5% market share.

Although Symantec was not listed as a leader in 1999 if their revenue is added to that of AXENT (acquired by Symantec in 2000), Symantec would have been ranked third with approximately $8.1 million in revenue with a 6% market share (See **Appendix L**).

Segments

The leaders can also be separated according to segments. The segments for encryption include:

- Encryption algorithms and tool kits

- File encryption applications

Encryption algorithms and tool kits is software that represents the enabling technologies for ecommerce systems. This is an important segment due to the nature of ecommerce demanding secure and trusted environments.

Worldwide Encryption Algorithm and Software Developer Kit Revenue by Vendor, 1997-1999 ($M)

	1997	1998	1999	1999 Share (%)	1998-1999 Growth (%)
RSA Security	27	39	51.2	53.9	31.3
Hitachi	-	-	10.3	10.8	NA
Certicom	0.8	1.5	6.5	6.8	333.3
Baltimore	0	3	4	4.2	33.3
IBM	1.4	2.2	2.6	2.7	16.0
Fujitsu	2.3	2.3	2.3	2.4	-0.4
F-Secure	0.4	0.5	1.3	1.3	150.0
RPK	0	0.1	1	1.1	880.4
Other international ISVs	4.4	5.2	6.7	7.1	28.3
Other international SVs	2	2.7	3.5	3.7	28.2
Other U.S. ISVs	5.9	3.9	5	5.3	28.7
Other U.S. SVs	0.3	0.5	0.7	0.7	30.0
Total	44.5	60.9	95.1	100.0	

Source IDC, 2000

File encryption applications include products such as Pretty Good Privacy (PGP) by Network Associates and DiskLock by Symantec. These applications allow the user to encrypt data on their hard drive making their data secure even if the system is stolen or compromised.

Worldwide File Encryption Application Revenue by Vendor, 1997-1999 ($M)

	1997	1998	1999	1999 Share (%)	1998-1999 Growth (%)
Data Fellows	6.7	9.5	11.3	29	18.4
Network Associates	7.4	8.6	7	18	-19.0
Symantec	1	2	5	12.9	150.0
AXENT Technologies	1.3	2.6	3.1	8	19.1
Hitachi	0	0	1.1	2.9	NA
Fujitsu	1	1	1	2.5	-0.4
NovaStor	0	0.6	0.6	1.5	0.0
IBM	0.2	0.4	0.5	1.2	16.0
Other international ISVs	3.6	4.3	5.5	14.1	28.3
Other international SVs	0.9	1.2	1.5	3.9	28.2
Other U.S. ISVs	2	1.3	1.7	4.3	28.7
Other U.S. SVs	0.3	0.5	0.7	1.7	30.0
Total	24.3	32	38.8	100	21.5

Source IDC, 2000

GEOGRAPHIC REGION

The North American market dominated the encryption market in 1999 with 53% of the revenue. Western Europe followed the North American market with 26% (See **Appendix M**).

OPERATING ENVIRONMENT

In 1999, market leadership belonged to Unix with $54 million in revenue, representing approximately 40% market share.

32-bit Windows operating environment came in second with $40 million in revenue and 30% market share (See **Appendix N**).

MARKET OUTLOOK

GEOGRAPHIC REGION

North America is predicted to lose market share from the 1999 level of 53% to an estimated 51% by 2004. Western Europe during this same time period is expected to increase from 26% to an estimated 31%. The other geographic regions are predicted to follow the same course as the North American region in losing their market share of revenues for the encryption market (See **Appendix M**).

OPERATING ENVIRONMENT

The dominant operating environment is forecasted to change by 2004. Although Unix leads the 1999 encryption market with $54 million in revenue, representing 40% market share, it is forecasted to lose a large percentage of the market ending 2004 with $32 million in revenue and 13% market share.

32-bit Windows is predicted to be the dominant operating environment in 2004 with $93 million in revenue and 39% market share.

IDC predicts that embedded and subsystems will be an up-and-coming market growing at a CAGR of 45% from 1999-2004. With a CAGR of 45%, Embedded and subsystems will own 18% of the market by 2004, reflecting $43 million in revenue.

Linux is also forecasted to capture market share by growing from approximately $0 to $33 million by 2004, passing Unix capturing 14% of the market (See **Appendix M**).

VENDORS

U.S. vendors controlled this market in 1999 with approximately 64% compared to international vendors with approximately 36% (See **Appendix O**).

SEGMENT

Encryption algorithm and developer tools are forecasted to grow at a CAGR of 12.5% increasing their percentage of market share by 1% to 66%. The file encryption applications are predicted to grow at CAGR of 11.5% (See **Appendix P**).

MARKET TRENDS

With the top five vendors controlling approximately 66% of the encryption market in 1999, consolidation is expected among the smaller vendors.

Security is a must in the world of ecommerce and encryption is what holds it all together. Thus, it is very important to build software using the strongest most well established encryption software obtainable. These software products must also be designed and built in such a way that allows upgrades to the cryptographic engines.

In the past the strength of the encryption in software limited U.S. vendors in their market expansion due to restrictions in U.S. export regulations. In January of 2000, the United States changed the encryption export regulations making it less restrictive. The major features of the new regulations include:

- "Retail" encryption products are widely exportable to all but certain "terrorist" nations though still subject to a government review and reporting requirements.
- Non-retail products are also exportable, subject to similar requirements, to most non-government users.
- Encryption products with less than 64-bits are freely exportable.
- Some non-proprietary source code is exportable to most countries after notice to the government.

While there are still laws limiting the encryption technology that U.S. companies may export, these new regulations help U.S. companies by allowing them to export stronger encryption technologies making them more competitive in international markets. The expiration of RSA patents will increase competition generated by all vendors but will be offset by the overall expansion of the market and growth of encryption enabled applications.

Encryption is gaining in importance in privacy products and services. Strong growth in applications like secure email and secure file transfer will continue into the future. Growth will also be stimulated through the passage of new regulations. One such regulation is the Health Insurance Portability and Accountability Act of 1996 (HIPAA). HIPAA is expected to stimulate demand for encryption products as well as other Internet security products, the extent of which will be determined by the final security ruling anticipated to be out by the end of 2001.

This final security rule requires all health plans, health care clearinghouses, and those health care providers to apply security standard to all health care information pertaining to an individual that is electronically maintained or electronically transmitted.[54] Small health plans have 36 months to comply from the date of the final ruling. All other health plans must comply within 24 months. In order to comply covered entities must ensure that:

- Any connection to the internet, or other external networks or systems, occurs through a gateway/firewall
- Strong authentication is used to restrict access to critical systems/business processes and highly sensitive data
- Assessments of vulnerability, reliability, and the threat environment are made at least annually.[55]

Encryption is becoming more recognized as a necessity on the Internet and as such has seen resurgence in growth beating out previous estimates for growth. The growth in encryption is closely related to the growth in technologies such as PKI, VPN, and secure socket layer (SSL). IDC predicts that the trend toward embedded encryption functionality will increasing be a driver of ecommerce.

INDUSTRY LEADERS

The following companies are the leaders and participants in the Internet security industry. These companies display some common characteristics including strength in: sales, sales growth, profit margin, net income growth, and return on equity. The purpose of this section is to profile the prominent players in each of the segments. These companies control a significant portion of the market. The accomplishments of these companies related to their superior financial performances are highlighted. After the leaders, smaller security firms that are doing well are profiled. Regional clustering occurs within the Internet security industry. As such, other Internet security companies operating within these high tech regions are profiled to show the pockets of clustering throughout the country. Consolidation has allowed leaders to gain a presence in many segments of the industry. Therefore, these companies are considered leaders in multiple segments, due mainly to the acquisition of smaller companies.

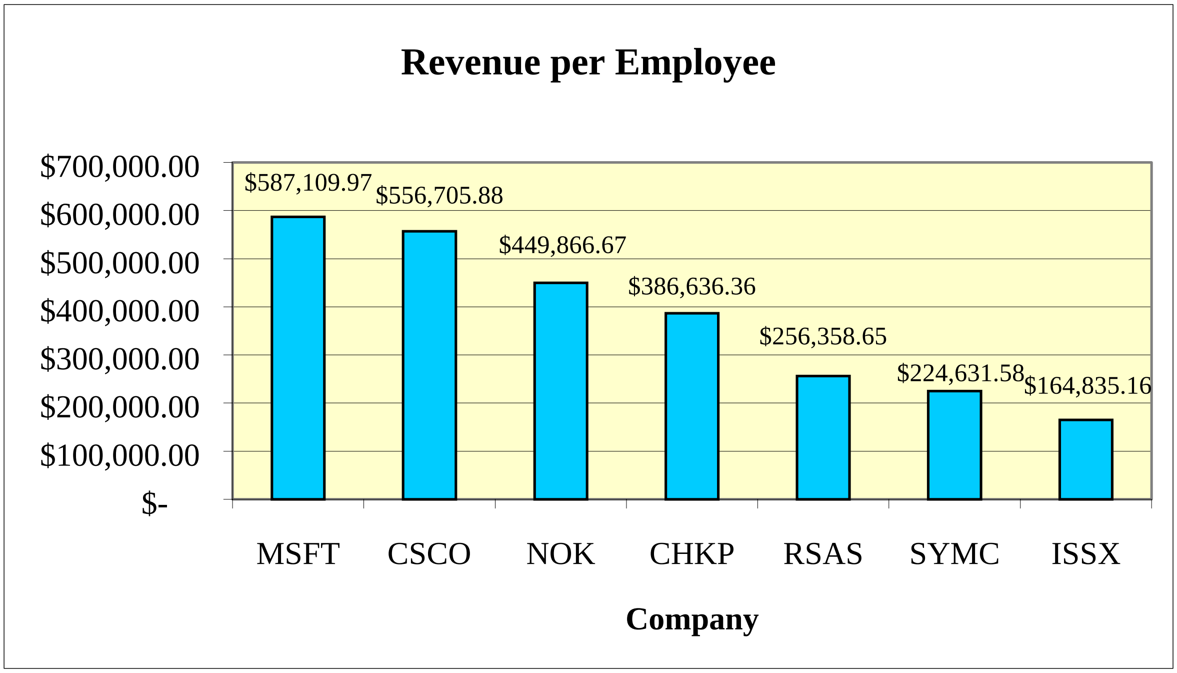
SUCCESS FACTORS

The big players profiled in the next section succeed financially because of their ability to accurately predict the movement of the market. They have experienced phenomenal growth during the past two fiscal years.

In our analysis of financial data from CompuStat of seven of the following eight companies, we found some similarities in regards to their cost structure and research and development costs. Their total costs before interest, taxes, and depreciation tended towards 70% - 80% of their sales. Their R&D was above 10% of revenues pretty consistently over the last 10 years. These companies are able to keep costs in line to consistently generate profits. R&D consistently makes these companies' products top of the line. Advertising expense was reported for most of these companies, so branding is occurring; however, there is no consistency within the seven companies we examined. Even advertising expense among other companies in the industry did not have any consistent percentage explaining any lack of success.

Consolidation plays an important role in the great successes of some of the following companies. Symantec, for example, recently acquired Axent. This expanded their operations and helped keep revenue healthy and net income in positive territory.

Another prevalent characteristic of these companies is their revenue per employee. The seven companies in the graph below had revenue of over $150,000 per employee. Microsoft and Cisco exceeded $500,000 per employee, but they are involved in significantly more markets. These levels of revenue per employee demonstrate effective workers. Other companies in IDC's leading companies also had revenue per employee as high as the seven we profile below. Since IDC's ranking is based on market share, this shows that leading companies with high market share have productive employees generating hundreds of thousands of dollars in revenue. The graph below displays each of the companies and their corresponding revenue per employee.



Source: http://www.thestandard.com/companies

LEADING COMPANIES

In researching companies, some clear leaders became evident. Their success comes from the way they do business and the economic prominence they each possess. Based on ROE, Profit Margin, and Sales growth, these companies stand out from the rest. These companies would be at the top of the list of whom Utah should know. Utah should look to these companies as major players in the security industry. In a few cases, the company with the most market share is not always the top performer. Perhaps this is an indication that the market share leaders will loose their market share in the future; as such the most financially successful are presented here.

Major National Security Companies

	Contact	Address	Phone	Website
Check Point (HQ - Israel)	Jerry Ungerman President	3 Lagoon Dr, Ste. 400 Redwood City, CA 94065	650/628-2000	www.checkpoint.com
RSA Security	Arthur Coviello President/CEO	36 Crosby Dr. Bedford, MA 01730	781/301-5000	www.rsa.com
Symantec	John Thompson President/CEO	20330 Stevens Creek Blvd. Cupertino, CA 95014	408/253-9600	www.symantec.com
Trend Micro (HQ - Tokyo, Japan)	Mike Conner President, North American Operations	10101 N De Anza Blvd, 2nd Floor Cupertino, CA 95014	408/257-1500	www.antivirus.com
Internet Security Systems	Thomas Noonan President/CEO	6303 Barfield Rd Atlanta, GA 30328	404/236-2600	www.iss.net
Microsoft	Steven Ballmer CEO Rick Belluzzo President/COO	One Microsoft Way Redmond, WA 98052	425/882-8080	www.microsoft.com
Cisco	John Chambers President/CEO	170 West Tasman Dr. San Jose, CA 95134	408/526-7208	www.cisco.com
Nokia	Sari Baldauf President Nokia Networks	6000 Connection Drive Irving, TX 75039	972/894-5000	www.nokia.com

CHECK POINT™
Software Technologies Ltd.

Check Point

	Fiscal	
	2000	**1999**
Sales	425.3	219.6
Net Income	221.2	95.8
Equity	549.3	292.5
Profit Margin	52.01%	43.62%
ROE	40.27%	32.75%
Sales Growth	93.67%	
Net Income Growth	130.90%	

US Headquarters: Redwood City, CA
Leader in: Firewall

Check Point Software is a clear leader in the firewall software industry. With a 2000 profit margin of 52%, they are very efficient in their operations. This number is significant since 1999 profit margin was 43.6%. Not only did they have a high profit margin, but sales are also up 93.7% over 1999 and net income is up over 130%. Check Point had over 40% as its return on equity indicating how well the company is performing for its investors. Part of this significant financial performance is due to the assistance from the Israeli government and different accounting laws; however, something is being done properly at this company with a market share of over 40%.[56]

Check Point's software products allow ISPs such as AT&T, GTE Internetworking, and UUNet to provide security as an outsourced service to their own customers. Gil Shwed founded Check Point Software because he wanted to create a firewall product that was powerful, but easy to use. Check Point's flagship product FireWall-1 was launched in 1994. In November 2000, IDC reported that the company had 41 percent market share in the firewall software category. Their market share increased almost ten points over the previous year.[57] Along with their software development, Check Point also markets and supports their security software solutions. These products aim to protect information from unauthorized access and interception through public connections like the Internet.[58] The company's Secure Virtual Network (SVN) architecture provides the infrastructure that enables secure and reliable Internet communications. SVN secures business-to-business (B2B) communications between networks, systems, applications, and users across the Internet, intranets, and extranets.[59]

Headquarters: Bedford, MA
Leader in: 3A Security[*] and Encryption

RSA Security		
	Fiscal	
	2000	1999
Sales	280.2	218.1
Net Income	205.8	183.8
Equity	481.0	611.0
Profit Margin	73.45%	84.27%
ROE	42.79%	30.08%
Sales Growth	28.47%	
Net Income Growth	11.97%	

RSA Security is a leader in the encryption market. Their sales in 2000 were up 28.5% over 1999 and their net income was up 12%. With such growth, they were able to achieve profit margins of 73.5% and 84.3% for 2000 and 1999 respectively. Looking at return on equity, RSA made a good return for investors of 42.8% and 30.1% for 2000 and 1999. RSA is seeing success, and it is evident through examination of the traditional financial measures.

RSA provides electronic security (e-security) solutions. The operations of the e-security solutions segment consist of the sale of software licenses, hardware, maintenance, and professional services through two product groups: enterprise solutions and developer solutions. Enterprise solutions include sales of RSA SecurID authenticators, RSA ACE server software, RSA Keon software, and maintenance and professional services. Developer solutions include sales of RSA BSAFE cryptographic software and protocol products, RSA Keon components, and maintenance and professional services. In addition, the company invests in e-businesses and other technology companies. During 2001, RSA acquired X-cert International, Inc. an independent, public-key infrastructure (PKI) company.[60]

Headquarters: Cupertino, CA
Leader in: Firewall, Anti-viral, and 3A Security

Symantec		
	Fiscal	
	2000	1999
Sales	853.6	745.7
Net Income	63.9	170.1
Equity	1,376.5	618.0
Profit Margin	7.49%	22.81%
ROE	4.64%	27.52%
Sales Growth	14.47%	
Net Income Growth	-62.43%	

Symantec is popular for its Norton line of anti-viral detection and repair software. They have software and services related to the anti-viral, firewall, and security markets. Their firewall business blossomed with their acquisition of Axent technologies, a recent IDC leader in the firewall software industry. Symantec's overall profit margin for 2000 and 1999 was 7.5% and 22.8%.

[*] Authentication, Authorization, and Administration

Their net income did fall in 2000, which explains the fall in profit margin, but their sales did increase 14.5%. Their return on book equity gave investors 4.6% and 27.5% for 2000 and 1999. They are in competition with Network Associates popular products such as McAfee, yet come out on top in these financial measures.

Symantec provides their content and network security solutions to individuals and enterprises. The company provides virus protection, firewall, virtual private network, vulnerability management, intrusion detection, remote management technologies, and security services to consumers and enterprises around the world through offices in 37 countries. Through their acquisition of Axent Technologies, Symantec now has a software development lab in American Fork, Utah. Their security services accounted for 40% of fiscal 2001 revenues; e-support, 33%; enterprise solutions, 27%; and professional services and other, nominal.[61]

US Headquarters: Cupertino, CA
Leader in: Anti-viral

Trend Micro		
	Fiscal	
	2000	**1999**
Sales	208.0	133.4
Net Income	45.0	21.0
Equity	197.8	169.4
Profit Margin	21.63%	15.74%
ROE	22.75%	12.40%
Sales Growth	55.92%	
Net Income Growth	114.29%	

Trend Micro is a Japanese company with a significant presence in the US. Their sales grew 55.9% between 1999 and 2000, with a net income growth of 114.3%. Their profit margins for the two years were 21.6% in 2000 and 15.7% in 1999. Their return on equity was 22.8% and 12.4% for 2000 and 1999 respectively.

Trend Micro Incorporated was established in 1989 to import and sell computer operating systems. It changed its name to the current format in 1996 after the company's shares were transferred to Trend Micro Incorporated (Taiwan). In 1998, the Trend Micro group was reorganized and the company bought shares of Trend Micro (Taiwan) and its related companies in the United States, South Korea, Germany, and Italy. It then became the parent company of the group. The company went public in August 1998. Trend Micro develops, markets, and supports integrated anti-virus software and management solutions for corporate computer systems and personal computers. PC client software accounted for 42% of 1999 unconsolidated revenues; internet server software, 31%; royalties from overseas subsidiaries, 16%; LAN server software, 10%; groupware server and other, 1%. Unconsolidated revenues accounted for 52.5% of 1999 consolidated revenues. In 1998 Trend Micro consolidated all its eleven subsidiaries, two in the United States and one each in Taiwan, South Korea, Italy, Germany, Australia, Brazil, France, Hong Kong and Malaysia. Overseas sales accounted for 56.4% of 1999 consolidated revenues.[62]

INTERNET SECURITY SYSTEMS™

Headquarters: Atlanta, GA
Leader in: 3A Security

Internet Security Systems		
	Fiscal	
	2000	1999
Sales	195.0	116.5
Net Income	18.3	7.5
Equity	188.4	155.2
Profit Margin	9.38%	6.44%
ROE	9.71%	4.83%
Sales Growth	67.38%	
Net Income Growth	144.00%	

Internet Security Systems is a leading player in the 3A Security market. Their sales grew over 67% from 1999 to 2000. This with their net income growth of 144% for the same time period shows impressive efficiencies. This efficiency is evident in the profit margin of 9.4% in 2000, up from 6.4% in 1999. Return on equity was 9.7 % for 2000, up from the 4.8% return they had in 1999.

Internet Security Systems (ISS) is a leading global provider of security management solutions for e-business. By offering the SafeSuite security software, comprehensive ePatrol monitoring services, and industry-leading expertise, ISS serves as its customers' trusted security provider protecting digital assets and ensuring the availability, confidentiality, and integrity of computer systems and information critical to e-business success. ISS' security management solutions protect more than 5,000 customers including 21 of the 25 largest US commercial banks, 9 of the 10 largest telecommunications companies, and over 35 government agencies. Founded in 1994, ISS is headquartered in Atlanta, GA and operates additional offices throughout North America, Asia, Australia, Europe and Latin America.[63]

Microsoft®

Headquarters: Redmond, WA
Leader in: Firewall

Microsoft		
	Fiscal	
	2000	1999
Sales	22,956.0	19,747.0
Net Income	9,421.0	7,785.0
Equity	41,368.0	28,438.0
Profit Margin	41.04%	39.42%
ROE	22.77%	27.38%
Sales Growth	16.25%	
Net Income Growth	21.01%	

Microsoft is a large player in many software markets and aims not to be left out of the security market. The corporation as a whole had a profit margin of 41% and 39.4% for 2000 and 1999 respectively. Their return on equity was 22.7% and 27.4% for 2000 and 1999. With sales growth of 16.3%, they were able to increase their net income 21% from 1999 to 2000. Microsoft continues to expand beyond the personal computer, moving into interactive television (WebTV), ecommerce services (electronic marketplace deal with Commerce One), television stations (MSNBC), and video game consoles (Xbox).[64] In February 2001, they announced an enterprise-level firewall and Web caching technology that is aimed purely at IT security uses. IDC ranked Microsoft third in the firewall segment with 10% market share. Their revenue from firewall products in 1999 was over $51 million.[65] Their Internet Security and Acceleration Server is a replacement for an entry-level proxy server package that they currently sell.[66] It is an extensible enterprise firewall and Web cache server that integrates with the Microsoft Windows 2000 operating system for policy-based security and accelerating and managing internetworking. It also provides two tightly integrated modes—a multi-layer firewall and a high-performance Web cache server. The firewall provides filtering at the packet, circuit, and application layer, inspection to examine data crossing the firewall, and control of access policy and routing of traffic. The cache improves network performance and end-user experience by storing frequently requested Web content. The firewall and cache can be deployed separately on dedicated servers or integrated on the same box.[67]

CISCO SYSTEMS

Cisco		
	Fiscal	
	2000	**1999**
Sales	18,928.0	12,154.0
Net Income	2,668.0	2,096.0
Equity	26,497.0	11,678.0
Profit Margin	14.10%	17.25%
ROE	10.07%	17.95%
Sales Growth	55.73%	
Net Income Growth	27.29%	

Cisco Systems is the worldwide leader in networking for the Internet. Cisco provides end-to-end networking solutions that customers use to build a unified information infrastructure of their own or to connect to someone else's network. An end-to-end networking solution is one that provides a common architecture that delivers consistent network services to all users. The broader the range of network services, the more capabilities a network can provide to users connected to it. Cisco is unique in its ability to provide all these elements, either by itself or together with partners.[68] The Cisco PIX Firewall series delivers strong security in an integrated hardware/software firewall appliance that offers superior performance of up to 500,000 simultaneous connections and nearly 1.7 Gigabits per second (Gbps) aggregate throughput. Cisco's PIX Firewall products span the entire user application spectrum, from cost-conscious desktop firewalls for remote offices to carrier-class gigabit firewalls for the most demanding enterprise and service provider environments.[69]

NOKIA
CONNECTING PEOPLE

Nokia		
	Fiscal	
	2000	**1999**
Sales	26,992.0	19,954.0
Net Income	3,499.0	2,601.0
Equity	9,604.0	7,446.0
Profit Margin	12.96%	13.03%
ROE	36.43%	34.93%
Sales Growth	35.27%	
Net Income Growth	34.53%	

The Nokia firewall appliance, which includes market-leading FireWall-1 software from Check Point Software Technologies, allows organizations to deploy a single, integrated solution, providing secure Internet communications and access control for networks ranging from carrier-class to regional-office environments. Nokia IP Security Solutions offer a high level of redundancy to maximize fault tolerance and ensure continuous Internet connectivity. Nokia, an acknowledged leader in wireless network infrastructure and IP Security Solutions, has broadened its network competency through a range of market-leading VPN solutions that provide reliable, secure, and scalable data network connectivity for sophisticated management of the end-user experience. With 44% market share in the high end VPN hardware market (Infonectics), Nokia extends its reputation with its line of integrated Firewall/VPN solutions. In addition to partnering with the market leading software vendor, Check Point Software Technologies to deliver an integrated Firewall/VPN solution, Nokia has designed its own dedicated VPN offering.[70]

OTHER PROMISING COMPANIES

NETSCREEN (PRIVATE)
Robert Thomas
President and CEO
350 Oakmead Parkway
Sunnyvale, CA 94085
408/730-6000
http://www.netscreen.com

NetScreen Technologies, Inc. is a new firewall appliance company making a dramatic advance into the Internet security market by delivering some of the industry's highest performance firewall/VPN solutions. Recently, IDC reported that NetScreen has the highest market share in the high-end firewall appliance market.[71] They are also ranked #2 in the low-end market and #3 in the mid-range market. The company's breakthrough ASIC-based (Application Specific Integrated Circuit) approach to security enables near wire-speed packet processing, ensuring full connection bandwidth by eliminating the performance bottlenecks associated with other legacy security products. NetScreen's products span a broad range of applications, from the first gigabit-speed security systems for Internet data centers and service providers (the NetScreen-1000) all the way to solutions for a single telecommuter (the NetScreen-5XP). Management of NetScreen's security systems and appliances is handled through NetScreen-Global PRO, a highly scalable software platform that enables easy deployment, provisioning and network control. The company's security solutions are available directly from NetScreen and through domestic and international VARs, distributors, service providers, and OEM partners. The company has received more than $53 million in funding to date.[72]

PALMCHIP CORPORATION (PRIVATE)

Jauher Zaidi, Chairman and CEO
Naished Vashi, President and COO
2595 Junction Ave., 2nd Floor
San Jose, CA 95134
408/952-2000
http://www.palmchip.com

Palmchip Corporation is a privately held, pre-IPO company funded primarily by venture capital. Jauher Zaidi, to develop a system-on-a-chip framework, which allows plug and play for IP integration, founded it in 1996. It is headquartered in San Jose, California, with an R&D facility in Loveland, Colorado, and sales offices worldwide. As a leader in the development and license of reusable, configurable processor platform semiconductor IP (intellectual property) building blocks for system-on-a-chip (SOC) solutions, Palmchip provides processor (ARC, ARM, MIPS) platforms, hardware/software, co-development environments, and configurable customization to the computing, digital consumer, mass storage, networking, portable and wireless communications, and semiconductor markets.[73] Palmchip Corporation is a developer and supplier of Systems-on-a-Chip solutions, including engineering services, reusable cores, mega cells, libraries and tools. Palmchip developed and implemented its CoreFrameT Architecture in embedded applications for mass storage, mobile phone, printing server, and Internet security devices. Palmchip positions itself as a Virtual ASIC Company.[74]

RAINBOW TECHNOLOGIES, INC. (PUBLIC)

Walter W. Straub,
Chairman, President, and CEO
50 Technology Drive
Irvine, California 92618
949/450-7300
http://www.rainbow.com

Founded in 1984, Rainbow Technologies is a leading provider of security solutions for the Internet and ecommerce. Rainbow applies its core technology to a variety of Internet applications from securing software, to the acceleration of secure communication for ecommerce and Virtual Private Networks (VPNs). Rainbow's products include secure Web server and VPN acceleration boards; anti-piracy and Internet software distribution solutions; PKI-based security solutions; voice, data and satellite security systems; and USB-based authentication tokens.[75]

Rainbow Tech		
	Fiscal	
	2000	1999
Sales	163.3	121.1
Net Income	14.4	8.1
Equity	139.7	97.9
Profit Margin	8.82%	6.69%
ROE	10.31%	8.27%
Sales Growth	34.85%	
Net Income Growth	77.78%	

SONICWALL, INC. (PUBLIC)

Sreekanth Ravi
President and CEO
1160 Bordeaux Drive
Sunnyvale, CA 94089-1209
408/745-9600
http://www.SonicWALL.com

Founded in 1991, SonicWALL, Inc. designs, develops, and manufactures comprehensive Internet security solutions that provide access security, value-added security services, and transaction security products for a broad range of markets, including: enterprise, service providers, ecommerce, government, education, and healthcare.

SonicWALL Internet security appliances have a worldwide install base of more than 165,000 units protecting millions of computer users. By integrating its line of high-performance, solid-state firewalls with value-added security services such as network anti-virus, virtual private networking (VPN), strong authentication using digital certificates, content filtering, and other security services, SonicWALL Internet security appliances deliver comprehensive security solutions. SonicWALL continues to develop strategic relationships with partners such as Cisco, 3COM, NetGear, and Network Associates. More than 8,000 resellers worldwide distribute the SonicWALL line of security solutions.[76]

SonicWALL		
	Fiscal	
	2000	1999
Sales	69.4	21.0
Net Income	8.7	0.2
Equity	435.8	60.8
Profit Margin	12.54%	0.95%
ROE	2.00%	0.33%
Sales Growth	230.48%	
Net Income Growth	4250.00%	

WATCHGUARD TECHNOLOGIES, INC. (PUBLIC)

Christopher Slatt, Chairman and CEO
James Cady, President and COO
505 Fifth Avenue South, Suite 500
Seattle, WA 98104
206/521-8340
http://www.watchguard.com

WatchGuard is a leading provider of dynamic, comprehensive Internet security solutions designed to protect enterprises that use the Internet for e-business and secure communications. They are a pioneer in the creation of the plug-and-play Internet security appliance and offer solutions for any size organization. The company's innovative LiveSecurity Service enables organizations and users to keep their security systems up-to-date through WatchGuard's broadcasts of threat responses, software updates, information alerts, expert advisories, support flashes and virus alerts over the Internet.[77]

Watch Guard		
	Fiscal	
	2000	**1999**
Sales	60.7	20.6
Net Income	(15.7)	(16.0)
Equity	172.4	32.2
Profit Margin	-25.86%	-77.67%
ROE	-9.11%	-49.69%
Sales Growth	194.66%	
Net Income Growth	nmf [*]	

[*] Not a Meaningful Figure

REGIONAL CLUSTERS

After looking into the many companies that operate in the Internet security industry, it is clear that these companies have the tendency to cluster together. The competition is heightened and ideas are shared. The typical high-tech areas are included in these clusters. Below are the descriptions of additional companies that are operating in the high-tech areas of New York, Massachusetts, California, Texas, and Washington. Other Internet Security companies headquartered outside the United States are not included in this compilation.

MASSACHUSETTS

AUTHENTICA, INC. (PRIVATE)
Lance Urbas
President and CEO
170 Tracer Lane
Waltham, MA 02451
781/487-2600
http://www.authentica.com

Authentica helps businesses successfully make the Internet a useful and reliable business tool. Authentica protects valuable intellectual property on the Internet with a line of products called Recall. The Recall products allow companies control over the use and distribution of the three most critical forms of digital content: e-mail, documents, and web pages. Authentica's products can prevent authorized recipients from printing or forwarding information without permission, revoke user access to information even after it's sent, and delete all distributed copies of information at some future date. Authentica makes sure information protection is a reality.[78]

NETEGRITY, INC. (PUBLIC)
Barry N. Bycoff
Chairman and CEO
52 Second Ave
Waltham, MA 02451
781/890-1700
http://www.netegrity.com

Netegrity is a provider of software solutions that securely manage e-business. Companies use Netegrity's products to control user access to e-business Web sites, easily create e-partnerships, and secure business-to-business transactions. These products enable companies to strengthen relationships with their customers and partners, create new revenue opportunities, and reduce the operational costs of managing complex e-business Web sites. Netegrity was the only vendor to be placed in the leader quadrant within Gartner's Magic Quadrant Report in November 2000. According to META Group, Netegrity owns 75% of the portal access-management tools market as reported in ComputerWorld, January 2001.[79]

Netegrity		
	Fiscal	
	2000	1999
Sales	54.0	12.7
Net Income	2.7	(5.5)
Equity	117.9	106.4
Profit Margin	5.00%	-43.31%
ROE	2.29%	-5.17%
Sales Growth	325.20%	
Net Income Growth	nmf	

NETWORK-1 SECURITY SOLUTIONS, INC.
(PUBLIC)
Murray Fish, CPA
President, CFO, and Secretary
Reservoir Place
1601 Trapelo Road
Waltham, MA 02451
781/522-3400
http://www.network-1.com

Network-1 is a supplier of Host Intrusion Prevention Systems for Windows-based enterprise clients and servers. Organizations that use the Network-1 software products build uncompromising security for their Internet, Intranet, and Extranet communication environments. Network-1's CyberwallPLUS Host Intrusion Detection Systems provide a robust, cost-effective means to harden Windows-based servers and workstations against attacks that originate both internally and externally. Based on an integrated architecture of packet filtering, packet inspection, and active intrusion detection, CyberwallPLUS does more than simply detect network tampering. It provides fine-grain network access controls and a powerful intrusion prevention system that recognizes network attacks. It stops attacks even before alerting the administrator and logging suspicious activity as evidence.[80]

Network 1		
	Fiscal	
	2000	1999
Sales	1.1	0.4
Net Income	(4.8)	(7.0)
Equity	4.2	2.2
Profit Margin	-436.36%	-1750.00%
ROE	-114.29%	-318.18%
Sales Growth	175.00%	
Net Income Growth	nmf	

SystemSoft Corporation
(*Under Chapter 11 since 1999; Subsidiary, Rocket Software since 2000*)
Two Apple Hill, Suite 204
Natick, MA 01760
508/651-0088
http://www.systemsoft.com
1999 Sales $8.3 million
(80.4% growth over 1998)

SystemSoft Corporation, subsidiary of Rocket Software, develops Windows Utilities software solutions. Their Windows NT solutions, CardWizard, and PowerProfiler/SE, have respectively earned Best of Breed status for PC Card Plug-n-Play and Advanced Power Management. Established in 1991, SystemSoft quickly became a market leader in the development of system-level software solutions. The company originally focused on the Original Equipment Manufacturers channel, pre-shipped software on equipment from the PC industry's top hardware vendors, including IBM, Toshiba, NEC, and Micron. Today, SystemSoft offers its own and other third-party products through multiple sales channels including: OEMs, direct to corporate, resellers, and direct to users. SystemSoft products are represented exclusively in Japan by Pacific SystemSoft KK, a subsidiary of Toyo Microsystems, and in all other Asian markets by Insyde Software.[81]

California

Other Internet Security Leaders

(According to IDC as of end of 1999)

	Contact	Address	Phone	Website
Network Associates (Firewall, Anti-Viral, Encryption)	George Samenuk President/CEO	3965 Freedom Circle Santa Clara, CA 95054	972/308-9960	www.nai.com
F-Secure (HQ - Finland) (Encryption)	Christopher Vargas President of US Subsidiary	675 North First St, 5th Floor San Jose, CA 95112 (North America HQ)	408/938-6700	www.fsecure.com
Hitachi America (HQ - Tokyo, Japan) (Encryption)	Yoshihiro Koshimizu President	2000 Sierra Point Pkwy Brisbane, CA 94005 (North American HQ)	650/589-8300	www.hitachi.com
Certicom (Encryption)	Rick Dalmazzi President/CEO	25801 Industrial Blvd Hayward, CA 94545	510/780-5400	www.certicom.com

Network Associates		
	Fiscal	
	2000	1999
Sales	745.7	683.7
Net Income	(102.7)	(159.9)
Equity	518.7	660.1
Profit Margin	-13.77%	-23.39%
ROE	-19.80%	-24.22%
Sales Growth	9.07%	
Net Income Growth	-35.77%	

Headquarters: Santa Clara, CA
Leader in: Firewall, Anti-viral

Network Associates is a leader in the firewall, anti-viral, and encryption markets. They have a wide presence and offer many products. The Santa Clara, California-based company is in competition with security software maker Symantec to be the leader in the data security market. Network Associates makes desktop software such as VirusScan, the Sniffer family of network monitoring and troubleshooting tools, and firewall applications. The company also offers consulting and support services (about 30% of sales). Network Associates sells its products directly and through distributors including Ingram Micro and Tech Data. Network Associates is building its Internet presence through its myCIO.com subsidiary and McAfee.com, of which Network Associates owns 81%. Together the application service providers represent 7% of sales.[82]

F-Secure		
	Fiscal	
	2000	1999
Sales	38.7	23.5
Net Income	(12.3)	(9.4)
Equity	35.0	44.4
Profit Margin	-31.78%	-40.00%
ROE	-35.14%	-21.17%
Sales Growth	64.68%	
Net Income Growth	30.85%	

US Headquarters: San Jose, CA
Leader in: Encryption

F-Secure develops applications that provide data encryption, firewall protection, wireless access to virtual private networks, and virus protection. Through its Security as a Service program, F-Secure targets Internet and application service providers with software and services that protect the transmission and storage of critical data. It also offers outsourced security management services through its Online Solutions subsidiary. Clients include Yahoo!, Nokia, and IBM. Founder and CEO, Risto Siilasmaa, owns 49.43% of F-Secure.[83]

HITACHI

US Headquarters: Brisbane, CA
Leader in: Encryption

Hitachi		
	Fiscal	
	2000	**1999**
Sales	77,956.0	65,928.7
Net Income	165.0	(2,800.0)
Equity	28,023.0	23,708.9
Profit Margin	0.21%	-4.25%
ROE	0.59%	-11.81%
Sales Growth	18.24%	
Net Income Growth	-105.89%	

Hitachi America makes products for the highly technical American. The wholly owned US subsidiary of Japanese electronics giant Hitachi, Ltd., makes and sells consumer electronics, computer systems, and semiconductor products. They market TVs, camcorders, VCRs, DVD players, and handheld PCs. Its line of information systems' products includes DVD-RAM, hard drives, and printers. Their involvement in the security industry is related to their iPlanet Portal Server, an open standard, Internet-based solution that allows organizations to provide access to applications and information through a highly secure enterprise web portal. iPlanet Portal Server enables any authorized user with a Java-based web browser to log on to the Hitachi America network anytime, anywhere for convenient access to the network information they need.[84]

certicom™

Headquarters: Hayward, CA
Leader in: Encryption

Certicom		
	Fiscal	
	2000	**1999**
Sales	12.0	4.2
Net Income	(17.9)	(20.2)
Equity	36.0	35.5
Profit Margin	-149.17%	-480.95%
ROE	-49.72%	-56.90%
Sales Growth	185.71%	
Net Income Growth	-11.39%	

Certicom is one of the leading encryption companies in the industry. Certicom makes sure no one can tap into wireless signals. The company develops digital encryption technologies that ensure secure communications between handheld computers, mobile phones, pagers, and other wireless devices. Certicom licenses its encryption technology and integration toolkits to such manufacturers as Motorola, Palm, and QUALCOMM, which integrate the technology into their own wireless applications. Certicom also offers a range of other services, including security analysis, design, and integration. In order to extend its secure communications offerings, the company is developing certificate authentication services (electronic signatures) and virtual private network applications for handheld devices.[85]

COUNTERPANE INTERNET SECURITY, INC. (PRIVATE)
Tom Rowley, President and CEO
19050 Pruneridge Ave
Cupertino, CA 95014
408/777-3600
http://www.counterpane.com

Entrepreneur, Tom Rowley, and security technologist and author, Bruce Schneier, to address the critical need for increased levels of security services, established Counterpane Internet Security, Inc. in 1999. Centered on a network of sophisticated Secure Operations Centers and staffed by expert security analysts, the Company provides 24/7 monitoring, as well as penetration detection, and response. Counterpane's Managed Security Monitoring services enable e-business to be conducted safely.[86]

CYLINK CORPORATION (PUBLIC)
William P. Crowell, President and CEO
3131 Jay Street
Santa Clara, CA 95404
408/855-6000
http://www.cylink.com

Cylink Corporation develops, markets, and supports a comprehensive family of secure e-business solutions that protect and manage the access, privacy, and integrity of information transmitted globally. The Company's products secure local-area networks (LANs), wide-area networks (WANs), and public packet-switched networks such as the Internet. Since 1983, Cylink has developed commercial products using public key technology to secure the world's largest corporations and organizations. Cylink serves Fortune 500 companies, multinational financial institutions, and government agencies worldwide.[87]

Cylink		
	Fiscal	
	2000	**1999**
Sales	68.1	59.7
Net Income	(35.4)	(16.4)
Equity	59.2	62.0
Profit Margin	-51.98%	-27.47%
ROE	-59.80%	-26.45%
Sales Growth	14.07%	
Net Income Growth	nmf	

LITRONIC, INC. (PUBLIC)
Kris Shah, Chairman and CEO
17861 Cartwright Road
Irvine, CA 92614
949/851-1085
http://www.litronic.com

Litronic provides organizations with the tools and knowledge base necessary to successfully deploy and manage scalable security through the use of public key infrastructure (PKI). Litronic's technologies enable users to leverage the Internet for electronic commerce, communications, and network access while protecting the integrity of digital transmissions and stored data. Litronic’s complete line of enterprise-wide security solutions enhances Internet and Intranet security with additional security features for file protection, user authentication, and remote access capabilities as required by today's organizations. Smart card devices enable individuals and organizations to easily deploy single user logon and hardware strength cryptography within a standards-based, public key infrastructure. In addition, Litronic focuses on developing applications designed to manage the security lifecycle process within the enterprise, enabling organizations to confidently deploy hybrid smart card and soft token systems. All of Litronic's products are designed with an open architecture to be algorithm, platform, application, and token independent to deliver scalable solutions that meet the needs of the individual organization.[88]

Litronic

	Fiscal	
	2000	**1999**
Sales	39.4	31.7
Net Income	(41.4)	(7.1)
Equity	6.5	47.9
Profit Margin	-105.08%	-22.40%
ROE	-636.92%	-14.82%
Sales Growth	24.29%	
Net Income Growth	nmf	

RAINFINITY (PRIVATE)
Olivier Helleboid, President and CEO
2740 Zanker Road, Suite 200
San Jose, CA 95134
877/724-6333
http://www.rainfinity.com

Founded in 1998, Rainfinity provides software for e-business infrastructure that ensures reliability, security, and speed. The company’s modular solutions provide high availability, performance scaling, and transparent recovery for the critical elements of e-business transactions, including security, web and application servers, and network connections. Rainfinity solutions are based on the unique RAIN (Reliable Array of Independent Nodes) software clustering technology developed at the California Institute of Technology in collaboration with NASA’s Jet Propulsion Laboratory and the Defense Advanced Research Projects Agency. Rainfinity solutions eliminate the performance bottlenecks, points of failure, and capacity limits at critical junctures in the Internet infrastructure. RainWall, a software-only cluster solution for Check Point firewalls and virtual private networks (VPNs), enables organizations to easily add more capacity and fault-tolerance to their firewall security layer. RainSLB, an intelligent, scalable high availability solution for web servers dynamically distributes traffic across web, FTP, application, and other servers to alleviate performance bottlenecks and improve availability during peak traffic loads.[89]

REDCREEK COMMUNICATIONS, INC. (PRIVATE)
Thomas J. Kilcoyne, CEO
RedCreek Communications, Inc.
3900 Newpark Mall Road
Newark, California 94560
888/745-3900
http://www.redcreek.com

RedCreek Communications enables companies to expand the borders of their enterprises without increasing the vulnerability of their information. RedCreek provides comprehensive, feature-rich integrated hardware and software Virtual Private Network (VPN) packages that ensure the privacy of information as it is transmitted across private and public networks.[90] RedCreek is dedicated to helping customers expand their networks without increasing their vulnerability by providing low-cost, high-speed, and easy to use network security products. RedCreek's Ravlin 3VPN ArchitectureTM and Ravlin product line excel at both secure point-to-point transmission of data between locations and across widely distributed enterprises encompassing remote offices, mobile users, and corporate headquarters. All Ravlin products offer drop-in installation and easy administration, IPsec standards-based implementation, interoperability with other network equipment, and low total cost of ownership.[91]

SANCTUM INC. (PRIVATE)
Peggy Weigle, CEO
2901 Tasman Drive, Suite 205
Santa Clara, CA 95054
408/855-9500
http://www.sanctuminc.com

Founded in 1997 and headquartered in Santa Clara, California, Sanctum, Inc. provides Web application security solutions. Sanctum software solutions provide automatic enforcement of intended business processes, ensuring the protection of core information and data. By detecting and defending against any unauthorized behavior, Sanctum protects customers against malicious cyber-criminal activity even if a site has unknown security holes or flaws. Sanctum's solutions can complete a company's security infrastructure, assure regulatory compliance, and create sustainable ROI. Sanctum's customers include industry leaders in finance, retailing, healthcare, government, and telecommunications. Privately held, Sanctum is funded by blue-chip venture capital firms and industry leaders including Sprout Group, Dell, Gemini Israel Funds, Fidelity Ventures, First Union eVentures Group, Mofet Israel Technology Fund, and Walden Israel.[92]

SECURE COMPUTING CORPORATION (PUBLIC)
John McNulty
Chairman and CEO
4810 Harwood Road
San Jose, CA 95124-5206
408/979-6100
http://www.securecomputing.com

Secure Computing is a global provider of e-business security products, delivering the strongest e-business access control, user authentication, and Web filtering solutions available. Their solutions can be customized to meet the needs of organizations of all sizes. Their customers include companies from the Fortune 50, application and Internet service providers, and government agencies. Together and individually, Secure Computing's comprehensive network security solutions--Sidewinder, SafeWord, and SmartFilter--help enable safe, secure extranets.[93]

Secure Computing		
	Fiscal	
	2000	**1999**
Sales	39.1	27.1
Net Income	(19.2)	(44.9)
Equity	30.6	15.3
Profit Margin	-49.10%	-165.68%
ROE	-62.75%	-293.46%
Sales Growth	44.28%	
Net Income Growth	nmf	

SECURIFY, INC. (PRIVATE)
Taher Elgamal
Chairman, President, and CEO
1157 San Antonio Road
Mountain View, CA 94043
650/812-9400
http://www.securify.com
2000 Sales $5 million

Securify is a leading provider of cost-effective e-Security technologies and solutions. Securify combines its own unique technology and expert services to provide customers the ability to achieve business objectives and maximize their network security investments. The Company offers two complementary suites of solutions—SecurVantage and Access Management Services.[94]

VERISIGN (PUBLIC)
Stratton Sclavos
President and CEO
487 East Middlefield Road
Mountain View, CA 94043
650/961-7500
http://www.verisign.com

VeriSign, Inc. is the world's largest provider of Internet trust services, supporting businesses and consumers from the moment they first establish an Internet presence through the entire lifecycle of ecommerce activities. Serving the largest base of business customers on the Internet, VeriSign offers domain name registration services, authentication, validation, and payment services to deliver on its mission to enable everyone, everywhere, to use the Internet with confidence. VeriSign serves as a gateway to establishing an online identity and Web presence, operating the definitive database of over 28.2 million Web addresses in .com, .net and .org on a powerful platform that is the world's de facto standard in Domain Name System (DNS) registry services. Responding to over 1.5 billion DNS look-ups daily, the powerful platform serves all of the world's domain name registrars and helps position VeriSign as a leading provider for secure high-volume transaction services. Customers of VeriSign benefit from the industry's most sophisticated managed digital certificate services, enabling them to leverage the company's infrastructure to deploy digital certificates for employees, customers, and partners. VeriSign also supports enterprise customers through a suite of solutions designed to manage their Internet presence, extranets, payment, and other ecommerce-related services.[95]

VeriSign		
	Fiscal	
	2000	**1999**
Sales	474.8	84.8
Net Income	(3,115.5)	4.0
Equity	18,470.6	298.4
Profit Margin	-656.17%	4.72%
ROE	-16.87%	1.34%
Sales Growth	459.91%	
Net Income Growth	-77987.50%	

TEXAS

Other Internet Security Leaders

(According to IDC as of end of 1999)

	Contact	**Address**	**Phone**	**Website**
Entrust (3A Security)	David Thompson Alberto Yepez Co-Presidents/CEO	4975 Preston Park Blvd, Ste 400 Plano, TX 75093	972/943-7300	www.entrust.com

Headquarters: Plano, TX
Leader in: 3A Security

Entrust		
	Fiscal	
	2000	**1999**
Sales	148.4	85.2
Net Income	(82.3)	5.9
Equity	674.1	103.2
Profit Margin	-55.46%	6.92%
ROE	-12.21%	5.72%
Sales Growth	74.18%	
Net Income Growth	-1494.92%	

Entrust (formerly Entrust Technologies) is a leading security company. Entrust's security software ensures the privacy of electronic communications and transactions across corporate intranets and the Internet. The Entrust tools automate the management of digital certificates (electronic passports that identify users) and monitor applications such as remote access and e-mail. Entrust also issues digital certificates through Entrust.net, offers systems integration services, and (through its 2000 purchase of enCommerce) offers software for managing e-business portals. The company sells to customers such as

Citibank, FedEx, and NASA. Telecom giant Nortel Networks owns almost 26% of Entrust.[96]

BINDVIEW DEVELOPMENT CORPORATION (PUBLIC)
Eric J. Pulaski, Founder, President, and CEO
5151 San Felipe, Ste. 2100
Houston, TX 77056
713/561-4000
http://www.bindview.com

BindView Corporation began in 1990 in Houston, Texas. Their initial product, developed in 1991, was a software solution designed to report on the security of PC-based networks. Over the last decade their product offerings have grown through development and acquisition. They are now a recognized leader as a provider of IT security and management solutions offering a suite of products for securing and administering today's most widely-used platforms and applications, such as Microsoft Windows and Exchange solutions, Novell NDS and eDirectory, UNIX, SAP, and OS/400 systems, as well as a solution for Internet Security. They are expanding the company continuously, and currently have offices throughout the United States and in Canada, Latin America, Europe, the Middle East, India, and Asia-Pacific.[97]

BindView		
	Fiscal	
	2000	**1999**
Sales	86.1	67.9
Net Income	(3.8)	7.0
Equity	92.3	81.8
Profit Margin	-4.41%	10.31%
ROE	-4.12%	8.56%
Sales Growth	26.80%	
Net Income Growth	-154.29%	

INFRAWORKS (PRIVATE)
Joyce Durst, CEO
Dr. George Friedman, CTO
504 Lavaca Street, Suite 1100
Austin, TX 78701
512/583-5000
http://www.infraworks.com

Founded in 1997 and privately held, Austin, Texas-based Infraworks Corporation is an emerging developer of infrastructure security software and technologies. With their suite of Digital Property Protection products and patented Active Security Technology, owners of digital assets can define and control the use of their creative and intellectual properties. Infraworks' InTether technology is the only solution available that protects data at its most vulnerable point - while in use.[98]

PENTASAFE SECURITY TECHNOLOGIES, INC. (PRIVATE)
Douglas J. Erwin, President and CEO
Park Towers North
1233 West Loop South Ste 1800
Houston, TX 77027
713/523-1992
http://www.pentasafe.com

PentaSafe Security Technologies, Inc. helps companies safely grow their businesses by providing complete security policy and infrastructure solutions that address security from a people, policy, and technology perspective. Unlike any other vendor, PentaSafe helps to educate the people within an organization to comply with information security policies and integrates each policy using best of breed security technology -- all designed to ensure maximum protection of information assets throughout a corporate enterprise. They offer security solutions for companies of all sizes, including policy management, auditing, vulnerability assessment, host-based intrusion detection, and best-practice security publications. PentaSafe offers security management solutions for operating systems, databases, web servers, firewalls, and applications including Windows 2000/NT, AS/400 or iSeries, UNIX, NetWare, JDEdwards WorldSoftware, Microsoft IIS, Apache, iPlanet, BEA WebLogic, CheckPoint FireWall-1, Cisco's NetRanger, Oracle, Sybase, and SQL. PentaSafe's solutions are used by thousands of auditing and security professionals worldwide, including 4 of the "Big 5" auditing firms and one-half of the Fortune 100.[99]

WASHINGTON

AVENTAIL CORPORATION (PRIVATE)
Evan Kaplan
President, CEO, Co-founder
808 Howell St., 2nd Floor
Seattle, WA 98101
206/215-1111
http://www.aventail.com

The Aventail.Net managed service securely connects people to applications over the Internet. They enable business partners and mobile employees to securely access an enterprise's Web and legacy applications, regardless of whether they are a supplier connecting from their own office or a consultant relying on a client's high-speed connection. This managed service delivers a single infrastructure - one place to enforce policy and one point of accountability - and simplifies the challenges of integrating people, processes, and technology. In the past, securely connecting people to applications over the Internet has involved a series of complex and on-going integration projects that include Web authorization, authentication, VPN, LDAP directory, call center packages, and provisioning systems. Often, each new user community has required additional work and IT resources, and created the potential for resource-intensive custom development projects. Organizations then face significant and unpredictable operating costs to make new applications accessible to new user communities. Aventail eliminates these frustrations for many companies.[100]

CYBERSAFE CORPORATION (PRIVATE)
Jim Cannavino, Chairman and CEO
Richard P. Fox, President and COO
1605 NW Sammamish Road
Issaquah, WA 98027-5378
425/391-6000
http://www.cybersafe.com
2000 Sales $14 million
(300% growth over 1999)

CyberSafe transactional security solutions address securing business processes to accelerate business growth by closing the gap between the risk and opportunity in the new economy. CyberSafe develops sophisticated, reliable, and comprehensive transactional security solutions that:

- Protect business-critical assets and enable customers to build and maintain the trust relationships integral to effective collaboration in distributed work environments
- Facilitate or augment the pursuit of corporate business objectives, with a focused understanding of electronic business initiatives
- Simplify the management of administration, configuration, and monitoring of internal and external attacks from a centralized console
- Reduce both financial and labor administration costs

CyberSafe is a leader in the development of transaction services that secure B2B and B2C financial transactions. CyberSafe has partnered with First Data Corp., among others, and has formed a joint venture with Certicom Corp. in order to successfully develop this technology. The completed solution will provide users a greater degree of security, privacy, and anonymity than traditional systems, while merchants will benefit with greatly reduced charge-back costs, transaction repudiation, and liability risk.[101]

NEW YORK

Other Internet Security Leaders

(According to IDC as of end of 1999)

	Contact	Address	Phone	Website
Computer Associates (Firewall, Anti-Viral, 3A Security)	Sanjay Kumar President/CEO	1 Computer Associates Plaza Islandia, NY 11749	631/342-6000	www.cai.com
IBM	Samuel Palmisano	New Orchard Rd Armonk, NY 10504	914/499-1900	www.ibm.com

Headquarters: Islandia, NY
Leader in: Firewall, Anti-viral, 3A Security

Computer Associates		
	Fiscal	
	2000	**1999**
Sales	4,198.0	6,103.0
Net Income	(591.0)	696.0
Equity	5,780.0	7,037.0
Profit Margin	-14.08%	11.40%
ROE	-10.22%	9.89%
Sales Growth	-31.21%	
Net Income Growth	-184.91%	

Charles Wang founded Computer Associates (CA) in 1976 as a joint venture with a Swiss company. His first product was a file organizer for IBM computers. By 1980 he had bought out his Swiss partners. CA went public in 1981. They now offer over 800 software products including a top rated firewall software product. They are the 3rd ranked independent software vendor behind Microsoft and Oracle. As of the end of 1999, IDC ranked them as the 2nd biggest firewall software vendor in the country. Computer Associates designs, develops, markets, licenses, and supports a range of integrated eBusiness computer software solutions. The solutions address all aspects of eBusiness process, information, and infrastructure management. The solutions are mainly focused on enterprise management, security, storage, transformation and integration, portal and knowledge management, and predictive analysis and visualization. The Company's products can be used on all major hardware platforms, operating systems, and application development environments for enterprise computing, to include, OS/390 from IBM, Windows NT from Microsoft, UNIX provided by Sun Microsystems Inc., Hewlett-Packard Company, IBM, Compaq Computer Corporation and Linux.[102]

Headquarters: Armonk, NY
Leader in: 3A Security

IBM		
	Fiscal	
	2000	**1999**
Sales	88,396.0	87,548.0
Net Income	8,093.0	7,712.0
Equity	20,624.0	20,511.0
Profit Margin	9.16%	8.81%
ROE	39.24%	37.60%
Sales Growth	0.97%	
Net Income Growth	4.94%	

IBM creates customer solutions through the use of advanced information technology. They offer a variety of solutions, which includes services, software and financing, development, manufacture, and sales of advanced information processing products. The company also provides solutions for computers and microelectronic technology, software, networking systems, and information technology-related services. These services include a review of a company's overall enterprise architecture to determine how it effectively isolates non-trusted, outside networks from gaining access to internal, trusted networks and systems and the security design of platforms (routers, firewalls, web servers, application servers, etc.) to determine if any functions provided by them could cause undesirable security exposures. They also test all components within the scope of a project in an attempt to gain unauthorized access to the internal network of a company from three perspectives: a low level solitary hacker, a small team of competent hackers, and an expert team of highly motivated hackers. They review the security management controls for the included components covering policy, organization, personnel, asset classification and control, physical security, access control, network and computer management, business continuity, system development and maintenance, and compliance. Finally, they report the strengths and weaknesses found in all of the above activities with recommendations for short and long-term improvements.[103] IBM's operations comprise three hardware product segments (Technology, Personal Systems and Enterprise Systems), a Global Services segment, a Software segment, a Global Financing segment, and an Enterprise Investments segment. Hardware sales accounted for 43% of 2000 revenues; global services, 38%; software, 14%; global financing, 4% and enterprise investments, 1%.[104]

UTAH INTERNET SECURITY INDUSTRY LANDSCAPE

Utah has a number of the assets that it needs to build a world class Internet Security regional industry within the State. Utah has strong colleges and universities that produce hundreds of Computer Science graduates each year. The State of Utah has taken steps to encourage the use and development of Internet security applications; for example, Utah enacted the first digital signature legislation, which recognized digital signatures as legally binding and gave digital document evidentiary weight.[105] Also, within the State of Utah there is a presence of promising Internet security start-ups that have the potential to develop into large successful firms.

UNIVERSITIES

Utah has a large pool of highly educated workers. Utah has the second highest percentage (90.7) of persons over twenty-five with a high school diploma or more. Utah is only behind the District of Columbia in higher education enrollment as a percentage of total state population with 7.6 percent.[106] Utah has strong universities, including the University of Utah, Brigham Young University, and Utah State University. It also has several colleges and technical schools. These schools produce graduates with specialized computer skills, positioning Utah to further develop an Internet security industry because it has a pool of computer science graduates and experienced software developers.

While Utah has a strong computer science program, it does not have a strong presence of management information systems (MIS) programs. MIS is the marriage of computer science and business. It is a mix of technical computer training and business training. Professionals with MIS skills are very valuable to software companies because they understand both business and technical issues. Thus they can help companies make sound business decisions about technology issues.[107]

GOVERNMENT

State government can play a significant role in the development of Internet security. In recent years the State of Utah has taken steps that have facilitated the growth of the of Internet security companies, specifically the authentication segment of the industry. From 1995 to 1998 Utah was ahead of all other states in authentication policy and legislature. Following is a list of digital firsts for Utah.

1995 - The Utah Digital Signature Act, Utah Code Annotated xx 46-3-101 to –504 was enacted in 1995. This legislation was the first to authorize commercial use of digital signatures. It governs the use of public-private key pair encryption and certification authorities and was designed to comport with various international and national standards that are already in place. Certification authorities are licensed by the Utah Department of

Commerce. The legislation also protects the subscriber's private key as property, and therefore its theft or unauthorized use is subject to criminal and civil liability.[108]

1997- Utah becomes the world's first government agency to declare a certification authority. Under a program aimed to make electronic communication and transactions more secure, the state of Utah entrusted a banking subsidiary to store and authenticate digital signatures. The license to be a "certificate authority" was the first of its kind to be granted by a state or federal body.[109]

1999 Governor Michael O. Leavitt signed Utah's Digital State legislation using iLumin's Internet security technology. The event marked one of the first times that digital signatures have been used for signing major, statewide legislation in the United States.[110]

2000 - Utah Uniform Electronic Transactions Act
The State passed legislation regarding the Uniform Electronic Transactions Act, which established criteria, procedures, and legal standards governing electronic transactions. The measure authorizes state agencies to make rules defining transactions that will and will not be conducted electronically. In relation to the electronic transactions act, another bill was passed that removes statutory barriers for the purpose of facilitating the electronic delivery of government services.[111]

These events have brought attention to the State of Utah. These actions also have encouraged the development of an Internet security market in Utah; first, by creating a market where digital documents can be used as legal documents thus making them useful in business processes; second, by making the State a large potential customer due to the volume of documentation that the State is involved in and the money that could be saved through the implementation of digital documents. Utah has been a leader among states in authentication policy and implementation. This has created a seedbed in which authentication technology has grown. Now there is a significant presence of authentication companies in Utah.

UTAH COMPANIES

Within Utah there is a significant presence of Internet security companies. Utah has a cluster of companies that are involved in the authentication segment of the Internet security industry. There are also companies in Utah that are involved in the firewall, encryption, and administration segments of the Internet security market.

The following companies are involved in the authentication segment: ARCANVS, Inc.; Digital Signature Trust; Ingeo Systems; iLumin; and User Trust, Inc. While each has a different business model and is trying to make money on different pieces of the value chain, they are all working towards the goal of providing government, business, and individuals with legal, secure online transactions via the Internet. (See Company profiles below for a description of each). These companies provide growth potential for a world-class authentication industry within Utah.

Internet security companies in Utah that are not primarily focused on authentication products include: Access Data Corp., EarthSpeak International, Novell, and Symantec. Access Data Corp. develops software applications for password recovery, secure data erasing, and computer crime tracing software. EarthSpeak International provides secure encrypted computer-to-computer communications via the Internet. Novell's Security Services provide applications that enable secure Internet and intranet data transfer. Symantec produces security management and firewall software, including intruder alert, enterprise security manager, and access control software. (See Company profiles below for description of each).

> *"Any company that thinks they are going to make money on digital signature technology alone is wrong… the maximum value will be in the application software."*
> Todd Romney, ARCANVS, Inc.

These companies are small, privately held, and most are losing money, but they have the potential to become large profitable companies. The Internet security market is in its infancy and companies are still trying to develop business models that are profitable. It is still to be seen which pieces of the value chain will add enough value to generate significant revenue and extract income over cost of development. Some feel that the Internet security technology itself will be become a commodity. What will add value is how the technology is packaged to meet the business needs of companies and the personal needs of consumers. Companies that focus on Internet security technology without developing tools that provide some tangible advantage (for example - being more secure while being fast and convenient, or saving money in paper cost and lowering the cost of doing business) will not become large successful companies.

Utah's Internet security companies have the potential to grow into large successful companies, depending on which direction the Internet security market moves, how these companies place themselves in the market, and the availability of capital to help them through their growth cycles.

UTAH COMPANY PROFILES

Access Data Corporation - Password recovery, secure data erasing, Internet and computer crime tracing software

Access Data Corp. has been doing business in the Internet and computer forensics and cryptography fields since 1987 and has established itself as the password recovery expert. Access Data has developed a trusted relationship with the Federal Government, state and local law enforcement, and corporate America. Access Data's tools have become standard for computer forensic investigators.

Access Data also develops software that securely erases sensitive documents. When sensitive documents or personal information are deleted from PCs, these files still reside in the systems free-space and can be accessed by others even after reformatting the hard drive.[112] Access Data's AcceSecureClean develops reliable and comprehensive protection to electronically shred personal information.

Sales: $2,500,000 - $4,999,999
EMPLOYEES: 12

Executives:
President, Senior Cryptographic Engineer - Eric Thompson

ARCANVS, Inc. - Authentication services, relying party services, application software/Web-based services, professional consulting and education services, and certificate authority and repository hosting

ARCANVS is a registration authority for digital certificates licensed under state statutes in Minnesota, North Carolina, Oregon, Utah and Washington. Arcanvs' registration authority network provides secure, supported access to its digital certificates. Arcanvs serves as a single-source for Public Key Infrastructure business solutions, providing, among other products, authentication services, relying party services, application software/Web-based services, professional consulting and education services, and certificate authority and repository hosting. Markets served include national notary associations, secretaries of state, notary networks, state county recorders' offices, software application vendors, and enterprises employing notaries. Notary enterprises include financial services, healthcare, and other business sectors.[113]

Arcanvs owns a patent on the Digital Notary process. All major business contracts, mortgages, law documents, and some healthcare documents require notarization, in which the notary public must witness the signing of such documents. With the Digital Notary process the notary public and the signing party meet and digital documents are signed digitally. The advantage of this process is that there is no paper involved, which saves handling cost because it is much faster than the traditional notary process and it can be transferred electronically. Arcanvs develops the components necessary for this process including the forms and the certificate management system software. Arcanvs is primarily a technology company, developing the tools necessary for the Digital Notary process. It is now developing software business solution applications that will enable companies to do the process of notarizing digitally, saving time and money.

Sales**:** $5,000,000 - $9,999,999
Employees: 50

Executives:
Owner - Greg Laird

VP Finance - Suzanne Wright
VP Human Resources - Chris Blair
VP Sales - Bob Ycmat
Director of Product Management - Todd Romney

Digital Signature Trust - Digital certificate solutions

Digital Signature Trust (DST) is a subsidiary of Zion's Bank Corporation. DST provides digital certificate solutions with the purpose of confirming identity online. Besides providing the technology for secure online transactions DST also uniquely provides solutions for risk management. DST is the leader in guaranteeing the identity of individuals and businesses in digital transactions. As a "trusted third party," DST provides outsourced digital certificate services that help companies integrate digital signatures into their e-business applications. DST also provides the highest level of risk management available through their warranty programs.[114]

DST has differentiated itself from other companies by focusing on becoming a company that businesses can trust. DST has purposefully defined itself as a subsidiary of Zion's Bank Corporation because banking is an industry which people trust to hold assets. DST out sources the actual digital certificate software and forms. Its goal is to become the "trusted third party" for transactions done in cyberspace.

Net Income (Loss) 1999: ($7.6) million
Employees: 50

Executives:
President & CEO - J. Scott Lowry
Senior VP of Operations - Don Johnson
Senior VP of Strategic Initiatives - Trell Rohovit
Senior VP of Sales & Marketing - Greg Worch
President, Financial Services - Scott Schrader
VP of Government Services - Keren Cummins
CTO - Yuriy Dzambasow
VP of Engineering - Randy Fox
VP of Legal, Policy, and Risk Management - Thomas J. Greco
VP of Marketing - Geoff Kahler
VP of Business Operations - Lorraine H. Orr
VP of Professional Services - Vishvas Patel
VP of Security - Johnny L. Sumners

EarthSpeak International - Secure Encrypted Communications

EarthSpeak International, LLC (ESI), which recently moved its headquarters to Utah, has developed patented peer-to-peer technology that enables secure encrypted voice or text communication over the Internet. ESI is the only company in the US that offers both voice and text encrypted ephemeral applications for consumers, business, and government.

ESI has delivered global encrypted Voice over Packet, Instant Messaging, and secure file transfer solutions since 1998. ESI specializes in encrypting communications for Ecommerce, armed forces, government organizations, legal and accounting practices, medical and educational institutions, corporate networks, dating services, chat rooms, or any situation where communication security is an issue.[115] ESI is a small company, but has the potential to become a thriving Utah business. EarthSpeak's Securiphone product offers business and government secure telephone communications at a cost much less than conventional long-distance calling.

Employees: 4

Executives:
VP of Business Development - Don Jackson

Ingeo Systems - Legally binding digital documents

Ingeo helps local governments and businesses work through electronic automation. It provides tools and services to automate the filing and recording of real estate and other legal records.

Ingeo's current products focus on lien releases –the most commonly recorded document type. Tools for loan originators allow them to digitally create, sign, notarize, and transmit legally binding documents. The corresponding systems at the county recorder's offices receive the incoming documents, validate them, and digitally endorse them before passing the documents electronically to their existing indexing and archive systems. Ingeo's future products will expand to include recording of other document types.

Ingeo participates in diverse digital recording standards initiatives at both state and national levels. The company was the first to adopt the digital recording standard put forth by Fannie Mae for electronic recording. Ingeo's core products are ePrepare and eRecord. ePrepare enables users to digitally create, sign, notarize, and transmit legally binding documents. eRecord allows county agencies to electronically receive, validate, and endorse incoming documents, integrating the information with existing indexing and archive systems.

Sales: $10,000,000 - $19,999,999
Employees: 30

Executives:
President - Todd Hougaard
VP Sales - Allyson Luekenga

iLumin - eBusiness enabler providing infrastructure technology and services for enforceable online transactions

iLumin is the first company to employ digital signatures, XML, and Web-enabled applications. iLumin's patent-pending, Web-based Digital Handshake technology enables industry and government to conduct end-to-end, fully automated enforceable online transactions in a paperless and legally binding way. iLumin develops software applications that execute the digital document process. In putting together a working end-to-end digital document service, iLumin partners with encryption and automated software forms companies. To carry this out iLumin has formed strategic and technology partnerships with industry leaders, including Deloitte & Touche, Trans Union, Digital Signature Trust, Entrust, VeriSign, Baltimore, Arcanvs, RSA Security and CBF Systems/VMP Mortgage Forms. Their customers are certificate authority companies, other businesses, and governments in need of legally binding digital documents. Their current clients include H&R Block Mortgage, Trans Union, Stewart Title, The Utah State Court System, and ManageMyMoney.com. [116]

Sales**:** $1,000,000- $2,499,999
Employees: 69

Executives:
Chairman of the Board - D. Brent Israelsen, J.D.
President & CEO - Steve Schneider
Chief Scientist - Bruce Eric Brown, Ph.D.
EVP, Chief Marketing Officer - Ben K. Gould, Jr.
EVP, CTO - David A. Ellison
EVP, Sales - Alex Karakozoff
Chief Administrative Officer - Lane Ward
VP of Finance - Craig Shields
SVP Service - Kevin Ash

Novell - Network and Internet security solutions

Novell's Security Services provide applications that enable secure Internet and intranet data transfer. Novell provides the following Security Services.

Novell's security suite helps businesses protect their systems and strengthen network borders, provides integrated protection against internal and external threats, and secures customer, partner, and employee Internet and remote access to company data, while improving Internet browsing efficiency.

Novell Certificate 2.0 is a free product that can be used to protect confidential information transmitted over the Internet. Novell Certificate Server 2.0 is the first fully directory-integrated public key infrastructure (PKI) solution for enterprises of all sizes. It enables network administrators to issue and manage digital certificates in-house, ensuring that data is secure while in transit both over the network and over the Internet.

Novell iChain 1.5 is a network directory solution that pairs industry-leading caching and directory technologies with optimized security, management, and community services.

Novell Cryptography Support Modules are implemented with the Novell International Cryptographic Infrastructure technology. By downloading and installing the appropriate module, NICI-based components (Novell Certificate Server, Novell SSL, Novell Single Sign-on, etc.) use an appropriate level of cryptography. This includes the use of unlimited strength cryptography or up to 56-bit DES/RC2/RC4 data encryption and 1024-bit RSA key management strength for worldwide users (where allowed by local law).[117]

2000 Sales: $1,161.7 million
Employees: 4,893

Executives:
Chairman - Mr. Eric E. Schmidt
President and CEO - Mr. Jack L. Messman
EVP and COO - Mr. Stewart G. Nelson
SVP and CFO - Mr. Ron Foster
Chief Scientist and Technology Officer - Mr. Drew Major
SVP and Chief Information Officer - Mr. Ken Anderson
SVP and General Counsel - Ms. Josephine T. Parry
SVP, Business and Corporate Development and CTO - Mr. Carl S. Ledbetter
SVP, Worldwide Sales - Mr. Richard A. Nortz
VP, Corporate Marketing - Mr. Darin Richins
VP, Operations - Mr. Brian Dudley
VP, Novell Customer Services - Mr. Michael Lyons
VP; General Manager, Net Directory Services - Mr. Paul Smart
VP; General Manager, Net Management Group - Mr. Craig H. Miller

Symantec - Security management and firewall software providing network security

Symantec, a leader in the Internet security market based in Cupertino, CA, purchased Axent Technologies in January 2001. With this purchase Symantec acquired a division of Axent, located in American Fork. Symantec now operates a software development lab with 115 employees in American Fork. This division of Symantec now produces security management and firewall software, including intruder alert, enterprise security manager, and access control software.

Division Employees: 115

Division Executives:
VP, Chief Technologist - Rob Clyde

VP of Engineering - Russ Stay

USERTrust, Inc. - provider of information privacy and security solutions that enable companies to migrate their core business processes onto the Internet.

USERTrust's products create an environment that is secure, private, and enables legally enforceable transactions. USERTrust's offering is interoperable, scaleable, and customizable to clients business needs and can transform business processes to a web-enabled enterprise.

USERTrust offers solutions to companies involved in the following markets: Real Estate, Healthcare, and Financial Services.[118]

Executives:
Chairman of the Board - Paul J. Toscano
President, CEO - Nicholas E. Hales
COO, Executive VP - John R. Merrill
VP Sales - Ross Reimann

Sales: $500,000 - $999,999
Employees: 4

RECOMMENDATIONS

The State of Utah can play a role in the development of an Internet security regional industry. We recommend the State take the following actions:

Recommendation #1: Work to maintain Utah's position as a leading state in the implementation of Internet security policy legislation. Law regulates many applications of Internet security products, and Utah should enact laws, which facilitate the development of the most progressive Internet security processes. In the late 1990s Utah was considered the most vanguard and active state in implementing Internet security policy and legislation.

Recommendation #2: Building upon the 2000 Utah Uniform Electronic Transactions Act, which authorizes State agencies to use digital processes for government transactions, the State should work to implement electronic documentation within its separate agencies. To do this the State must first educate government agencies about the benefits of electronic documentation and second, mandate the use of or create incentives for the use of electronic documentation. The State should use the technology of local companies with the purpose of promoting the technology of these companies and to save paper costs.

Recommendation #3: Assign a high level State executive as a champion of State Internet security policy and implementation. Dave Moon, Utah's former chief information officer, advocated the development of Internet security policy and legislation. Utah needs an active supporter of Internet security.

Universities

Recommendation #4: Coordinate efforts with State universities to instigate a new Internet security program within the computer science and electrical engineering programs. The State should work to attract top computer science, computer engineering, and mathematics professors to form an Internet security program, which specializes in training students to work at companies involved in developing Internet security products.

Recommendation #5: Work with State universities to build up the Management Information Systems (MIS) programs. To do this the State should work to enlarge current MIS programs at state universities and attract MIS specialists. MIS skills are crucial for the successful management of technology companies and to bridge the gap between top management and technology developers.

Building Up Utah Internet Securities Companies

Recommendation #6: Facilitate the expansion of Utah's Internet security companies through their pre-IPO growth cycles by helping them obtain second and third round venture capital. Most of the capital available in Utah is seed capital, which helps companies through in their start-up stages. The State needs to help increase the amount of capital available by raising and attracting venture capital.

Recommendation #7: Encourage coordinated efforts of State university programs and Utah's Internet security companies by making Internet security a focus of the Centers of Excellence program and creating a non-profit incubator organization. Such an incubator would be located at a State university and set up for the purpose of developing Internet security and other technology-based companies. Such an incubator would assist start-ups by providing management resources and capital access, training management in entrepreneurial skills, and promoting tech transfers and joint ventures.

Recommendation #8: Promote the flow of ideas between Utah's Internet security companies by sponsoring industry forums. These forums should involve Utah companies, university faculty, and key State officials. The main goal of such a forum would be to encourage collaboration between Utah companies.   This would also promote a more open business environment, the flow of ideas, and increased personal contact between key players in Utah's Internet technology industry.

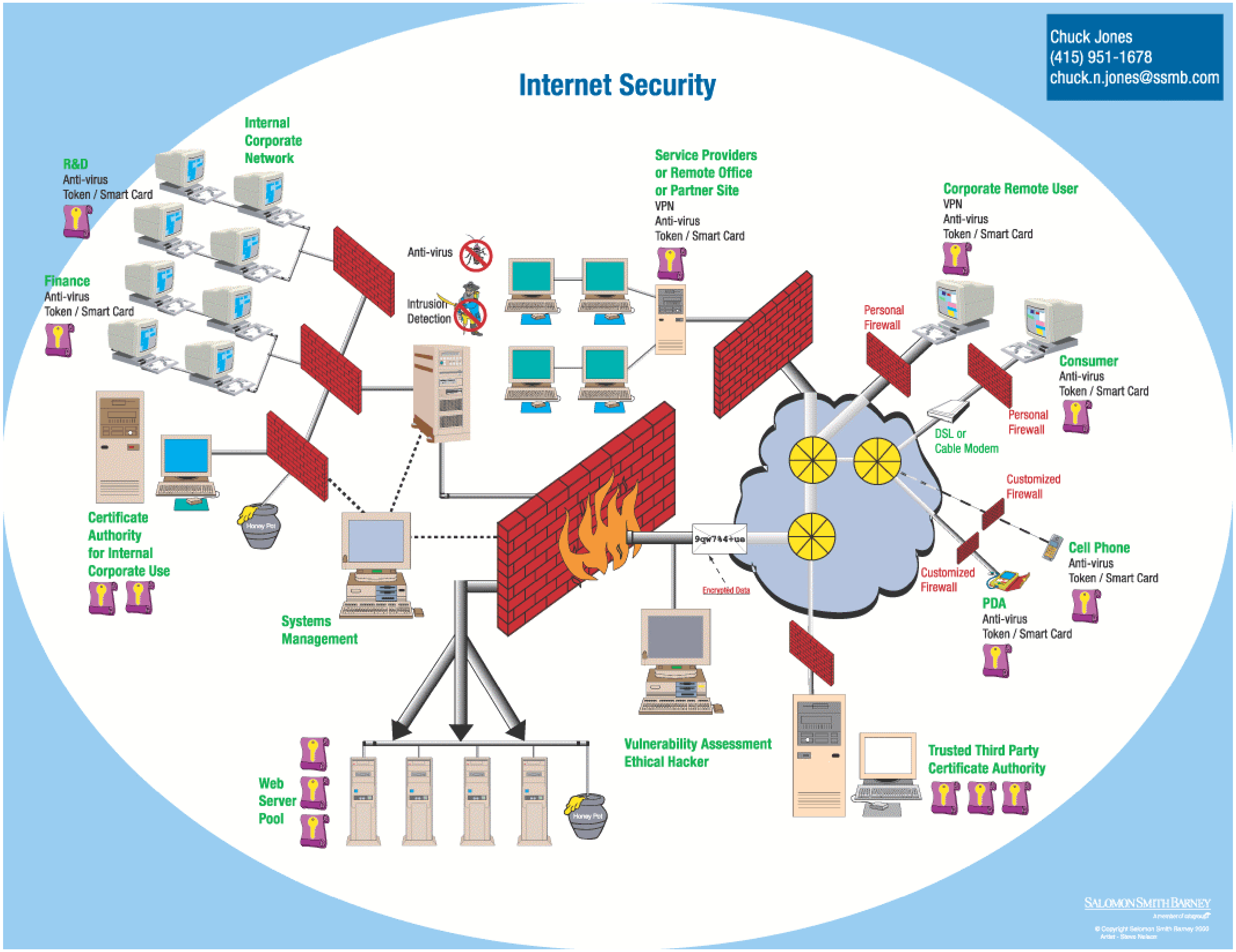
Recommendation #9: Use the Olympics as an opportunity to connect Utah's Internet security companies with potential clients, suppliers, leading Internet security companies, professional business services, and venture capital; ultimately, this will bring together valuable parts of the technology development model. The State should host these networking events giving invitees the opportunity to participate in the Olympic events in some way.

Focused Recruiting Activities

Recommendation #10: Work to attract encryption companies such as RSA Security, F-Secure, and Symantec. Utah has a significant presence of authentication companies. The important pieces of the value chain include certificate authorities, form developers, certificate management system software, and encryption technology developers (See Page 31). Utah has a certificate authority, form developers, and application developers, but lacks encryption developers. Utah should attract an encryption company to build a complete network of the authentication supply chain. Symantec already has a location in American Fork and the State would do well to form a relationship with this company.

Recommendation #11: Work to attract a company that develops firewall appliances, such as NetScreen, Nokia, WatchGuard, or SonicWALL. The firewall appliance segment is poised to be one of the fastest growing segments of the Internet security industry. Also, firewall appliances will complement the authentication that is being developed within state.

Appendix A: Internet Security Industry



Appendix B: Glossary of Terms

Glossary (obtained from http://www.setsolutions.com/security.htm and other endnoted sources)

Abuse of Privilege: When a user performs an action that they should not have, according to organizational policy or law.

Access Authorization: Permission granted to users, programs or workstations.

Access Control: A set of procedures performed by hardware, software and administrators to monitor access, identify users requesting access, record access attempts, and grant or deny access.

Advanced Encryption Standard (AES): An encryption algorithm for securing sensitive but unclassified material by US Government agencies and, as a likely consequence, may eventually become the de facto encryption standard for commercial transactions in the private sector.[119]

Algorithm: A mathematical procedure or formula for solving a problem.[120]

Anonymous FTP: A guest account, which allows anyone to login to the FTP Server. It can be a point to begin access on the host server.

ANSI: The American National Standards Institute. Develops standards for transmission storage, languages and protocols. Represents the United States in the ISO (International Standards Organization).

Application Level Gateway [Firewall]: A firewall system in which service is provided by processes that maintain complete TCP connection state and sequencing. Application level firewalls often re-address traffic so that outgoing traffic appears to have originated from the firewall, rather than the internal host.

Asymmetric Encryption: The use of public and private keys in the encryption of data.

Authentication: The process of establishing the legitimacy of a node or user before allowing access to requested information. During the process, the user enters a name or account number (identification) and password (authentication).

Authentication Tool: A software or hand-held hardware "key" or "token" utilized during the user authentication process. See key and token.

Authentication Token: A portable device used for authenticating a user. Authentication tokens operate by challenge/response, time-based code sequences, or other techniques. This may include paper-based lists of one-time passwords.

Authorization: The process of determining what activities are permitted. Usually, authorization is in the context of authentication. Once you have authenticated a user, the user may be authorized different access or activity.

Back Door: An entry point to a program or a system that is hidden or disguised, often created by the software's author for maintenance. A certain sequence of control characters permits access to the system manager account. If the back door becomes known, unauthorized users (or malicious software) can gain entry and cause damage.

Bandwidth: Capacity of a network or data connection, often measured in kilobits/second (kbps) for digital transmissions.

Bastion Host: A system that has been hardened to resist attack at some critical point of entry, and which is installed on a network in such a way that it is expected to come under attack. Bastion hosts are often components of firewalls, or may be 'outside" Web servers or public access systems. Generally, a bastion host is running some form of general-purpose operating system (e.g., LNIX, VMS, WNT, etc.) rather than a ROM-based or firmware operating system.

Biometric Access Control: Any means of controlling access through human measurements, such as fingerprinting and voiceprinting.

Challenge/Response: A security procedure in which one communicator requests authentication of another communicator, and the latter replies with a pre-established appropriate reply.

Certification Authority: A CA (certificate authority) is an authority in a network that issues and manages security credentials and public keys for message encryption. As part of a public key infrastructure(PKI), a CA checks with a registration authority (RA) to verify information provided by the requestor of a digital certificate. If the RA verifies the requestor's information, the CA can then issue a certificate.[121] A CA is also used by a recipient of a document that wishes to authenticate the sender of the message through use of the supposed sender’s public key.

Ciphertext: An encrypted message

Client/Device: Hardware that retrieves information from a server.

Coded File: In encryption, a coded file contains unreadable information.

Computer Security: Technological and managerial procedures applied to computer systems to ensure the availability, integrity and confidentiality of information managed by the computer system.

Cryptanalysis: The art of breaking ciphers.

Cryptographic Checksum: A one-way function applied to a file to produce a unique "fingerprint" of the file for later reference. Checksum systems are a primary means of detecting file system tampering on UNIX.

Cryptography: The art or science of keeping messages secret.

Cryptology: The branch of mathematics that studies the mathematical foundations of cryptographic methods.

Data at Rest: A data store or in other words information stored at a physical location. Data at rest is opposite of the term "data in motion" which refers to data that is in transit. Data at rest might contain data about customers, students, customer orders, or supplier invoices.[122]

Data Driven Attack: A form of attack in which the attack is encoded in innocuous-seeming data, which is executed by a user or other software to implement an attack. In the case of firewalls, a data driven attack is a concern since it may get through the firewall in data form and launch an attack against a system behind the firewall.

Data Encryption Standard: An encryption standard developed by EBM and then tested and adopted by the National Bureau of Standards. Published in 1977, the DES standard has proven itself over nearly 20 years of use in both government and private sectors.

Data in Motion: Data (e.g. credit card information, email messages) that has left the originating location and is still in transit to an end location. Data in motion occurs in-between users and is the opposite of "data at rest."

Data Store: A place where data is stored; data at rest. A generic term that includes databases and flat files.[123]

Decode: Conversion of encoded text to plain text through the use of a code.

Decrypt: Conversion of either encoded or enciphered text into plaintext.

Digital Certificate: An electronic "credit card" used to establish credentials when doing business or other transactions on the Web. Issued by a certification authority (CA), it contains the senders name, a serial number, expiration dates, a copy of the certificate holder's public key (used for encrypting messages and digital signatures), and the digital signature of the certificate-issuing authority so that a recipient can verify that the certificate is real. Some digital certificates conform to a standard, X.509. Digital certificates can be kept in registries so that authenticating users can look up other users' public keys.[124]

Digital Signature: An electronic signature (not to be confused with a digital certificate) that can be used to authenticate the identity of the sender of a message or the signer of a document, through the use of public key encryption.[125] The sender signs the document with a private key and the recipient verifies the sender via the sender's public key, which is attainable through a certification authority.

E-mail Bombs: Code that when executed sends many messages to the same address(s) for the purpose of using up disk space and/or overloading the E-mail or web server.

Encrypting Router: See Tunneling Router and Virtual Network Perimeter.

Encryption: The process of scrambling files or programs, changing one character string to another through an algorithm (such as the DES algorithm). There are two distinct types of encryption algorithm:

- single key or symmetric encryption; and
- public key or asymmetric encryption.

End-to-End Encryption: Encryption at the point of origin in a network, followed by decryption at the destination.

Enterprise: In the computer industry, an enterprise is an organization that uses computers. A word was needed that would encompass corporations, small businesses, non-profit institutions, government bodies, and possibly other kinds of organizations. The term enterprise seemed to do the job. In practice, the term is applied much more often to larger organizations than smaller ones.[126]

ERP: An acronym for Enterprise Resource Planning systems that permit organizations to manage resources across the enterprise and completely integrate manufacturing systems.

Extranet: A private network that uses the Internet protocol and the public telecommunication system to securely share part of a business's information or operations with suppliers, vendors, partners, customers, or other businesses. An extranet can be viewed as part of a company's intranet that is extended to users outside the company. It has also been described as a "state of mind" in which the Internet is perceived as a way to do business with other companies as well as to sell products to customers.[127]

Firewall: A system or combination of systems that enforces a boundary between two or more networks.

Flooding programs: Code which when executed will bombard the selected system with requests in an effort to slow down or shut down the system.

Gateway: A network point that acts as an entrance to another network. On the Internet, a node or stopping point can be either a gateway node or a host (end-point) node. Both the computers of Internet users and the computers that serve pages to users are host nodes. The computers that control traffic within your company's network or at your local Internet service provider (ISP) are gateway nodes.[128]

Generic Utilities: General purpose code and devices; i.e., screen grabbers and sniffers that look at data and capture information like passwords, keys and secrets.

Global Security: The ability of an access control package to permit protection across a variety of mainframe environments, providing users with a common security interface to all.

Granularity: The relative fineness or coarseness by which a mechanism can be adjusted.

Hack: Any software in which a significant portion of the code was originally another program.

Hacker: Those who are intent upon entering an environment to which they are not entitled. The hacker is characterized by their motives (e.g., pranksters, fame seekers, educational, criminals, extortionists, saboteurs, protesters, ideological). Usually iterative techniques escalate to more advanced methodologies and the use of devices to intercept the communications property of another.

Hashing: The process of computing a value that is message specific in order to verify to the recipient that the message remained unaltered in transmission.

Host: 1) In Internet protocol specifications, the term "host" means any computer that has full two-way access to other computers on the Internet. A host has a specific "local or host number" that, together with the network number, forms its unique IP address. If you use Point-to-Point Protocol to get access to your access provider, you have a unique IP address for the duration of any connection you make to the Internet and your computer is a host for that period. In this context, a "host" is a node in a network. 2) A computer with a Web server that serves the pages for one or more Web sites. A host can also be the company that provides that service, which is known as hosting.[129]

Host-based Security: The technique of securing an individual system from attack. Host-based security is operating system and version dependent.

Hybrid Gateways: An unusual configuration with routers that maintain the complete state of the TCP/IP connections or examine the traffic to try to detect and prevent attack [may involve baston host]. If very complicated it is difficult to attach; and, difficult to maintain and audit.

"In the wild" virus: A virus that is prevalent across networks and is infecting host machines.

Insider Attack: An attack originating from inside a protected network.

Internet (The Beginning): The Internet had its roots in early 1969 when the ARPANET was formed. ARPA stands for Advanced Research Projects Agency (which was part of the U.S. Department of Defense). One of the goals of ARPANET was research in distributed computer systems for military purposes. The first configuration involved four computers and was designed to demonstrate the feasibility of building networks using computers dispersed over a wide area. The advent of OPEN networks in the late 1980's required a new model of communications. The amalgamation of many types of systems into mixed environments demanded better translator between these operating systems and a non-proprietary approach to networking in general. Telecommunications Protocol/Internet Protocol {TCP/IP) provided the best solutions to this.

Internet (TOM): A web of different, intercommunicating networks funded by both commercial and government organizations. It connects networks in 40 countries. No one owns or runs the Internet. There are thousands of enterprise networks connected to the Internet, and there are millions of users, with thousands more joining every day.

Intranet: A private network that is contained within an enterprise. It may consist of many interlinked local area networks and also use leased lines in the wide area network. Typically, an intranet includes connections through one or more gateway computers to the outside Internet. The main purpose of an intranet is to share company information and computing resources among employees. An intranet can also be used to facilitate working in groups and for teleconferences.[130]

Intrusion Detection: Detection of break-ins or break-in attempts either manually via software expert systems that operate on logs or other information available on the network.

IP Sniffing: Stealing network addresses by reading the packets. Harmful data is then sent stamped with internal trusted addresses.

IP Spoofing: An attack whereby an active, established, session is intercepted and co-opted by the attacker. EP Splicing attacks may occur after an authentication has been made, permitting the attacker to assume the role of an already authorized user. Primary protections against IP Splicing rely on encryption at the session or network layer.

Key: In encryption, a key is a sequence of characters used to encode and decode a file. You can enter a key in two formats: alphanumeric and condensed (hexadecimal). In the network access security market, "key" often refers to the "token," or authentication tool, a device utilized to send and receive challenges and responses during the user authentication process. Keys may be small, hand-held hardware devices similar to pocket calculators or credit cards, or they may be loaded onto a PC as copy-protected, software.

Least Privilege: Designing operational aspects of a system to operate with a minimum amount of system privilege. This reduces the authorization level at which various actions are performed and decreases the chance that a process or user with high privileges may be caused to perform unauthorized activity resulting in a security breach.

Local Area Network (LAN): An interconnected system of computers and peripherals, LAN users share data stored on hard disks and can share printers connected to the network.

Logging: The process of storing information about events that occurred on the firewall or network.

Mobile Code: A program downloaded from the Internet that runs automatically on a computer with little or no user interaction.

Network Computer (NC): A "thin" client hardware device that executes applications locally by downloading them from the network. NCs adhere to a specification jointly developed by Sun, IBM, Oracle, Apple and Netscape. They typically run Java applets within a Java browser, or Java applications within the Java Virtual Machine.
Network Computing Architecture: A computing architecture in which the client dynamically downloads components from the network into the client device for execution. The Java programming language is at the core of network computing.

Network-Level Firewall: A firewall in which traffic is examined at the network protocol packet level.

Network Worm: A program or command file that uses a computer network as a means for adversely affecting a system's integrity, reliability or availability, a network worm may attack from one system to another by establishing a network connection. It is usually a self-contained program that does not need to attach itself to a host file to infiltrate network after network.

One-Time Password: In network security, a password issued only once as a result of a challenge-response authentication process. Cannot be "stolen" or reused for unauthorized access.

Operating System: System software that controls a computer and its peripherals. Modern operating systems such as Windows 95 and NT handle many of a computer’s basic functions.

Password: A secret code assigned to a user. A@ known by the computer system. Knowledge of the password associated with the user ID is considered proof of authorization. (See One-Time Password.)

PIN: In computer security, a personal identification number used during the authentication process. Known only to the user. (See Challenge/Response, Two-Factor Authentication.)

Plaintext: Data that is not encrypted in transmission. Also know as cleartext.

Policy: Organizational-level rules governing acceptable use of computing resources, security practices, and operational procedures.

Private Key: In encryption, one key (or password) is used to both lock and unlock data. Compare with public key.

Protocols: Agreed-upon methods of communications used by computers.

Proxy: 1) A method of replacing the code for service applications with an improved version that is more security aware. Preferred method is by "service communities", i.e. Oracle, rather than individual applications. Evolved from socket implementations. 2) A software agent that acts on behalf of a user. Typical proxies act as an intermediaries between a workstation user and the Internet accepting a connection from a user, making a decision as to whether or not the user or client IP address is permitted to use the proxy, perhaps does additional authentication, and then completes the connection on behalf of the user to a remote destination.

Public Key: In encryption a two-key system in which the key used to lock data is made public, so everyone can "lock." A second private key is used to unlock or decrypt. A public key is also used to authenticate a sender's digital signature.

Public Key Infrastructure: Algorithms that enable users of a basically unsecured public network such as the Internet to securely and privately exchange data and money through the use of a public and a private cryptographic key pair that is obtained and shared through a trusted authority. The public key infrastructure provides for a digital certificate that can identify an individual or an organization and directory services that can store and, when necessary, revoke the certificates.[131]

Registration Authority: An RA (registration authority) is an authority in a network that verifies user requests for a digital certificate and tells the certificate authority (certificate authority) to issue it. RAs are part of a public key infrastructure (public key infrastructure), a networked system that enables companies and users to exchange information and money safely and securely. The digital certificate contains a public key that is used to encrypt and decrypt messages and digital signature.[132]

Remote Access: The hookup of a remote computing device via communications lines such as ordinary phone lines or wide area networks to access network applications and information.

Risk Analysis: The analysis of an organization's information resources, existing controls and computer system vulnerabilities. It establishes a potential level of damage in dollars and/or other assets.

Rogue program: Any program intended to damage programs or data. Encompasses malicious Trojan Horses.

Router: A device or, in some cases, software in a computer, that determines the next network point to which a packet should be forwarded toward its destination. The router is connected to at least two networks and decides which way to send each information packet based on its current understanding of the state of the networks it is connected to. A router is located at any gateway (where one network meets another), including each Internet point-of-presence. A router is often included as part of a network switch.[133]

RSA: A public key cryptosystem named by its inventors, Rivest, Shamir and Adelman, who hold the patent.

Scalability: The ability to expand a computing solution to support large numbers of users without impacting performance.

Screened Host Gateway: A host on a network behind a screening router. The degree to which a screened host may be accessed depends on the screening rules in the router.

Screened Subnet: An isolated subnet created behind a screening router to protect the private network. The degree to which the subnet may be accessed depends on the screening rules in the router.

Screening Router: A router configured to permit or deny traffic using filtering techniques; based on a set of permission rules installed by the administrator. A component of many firewalls usually used to block traffic between the network and specific hosts on an IP port level. Not very secure; used when "speed" is the only decision criteria.

Server: In general, a server is a computer program that provides services to other computer programs in the same or other computers. The computer that a server program runs in is also frequently referred to as a server (though it may contain a number of server and client programs). In the client/server programming model, a server is a program that awaits and fulfills requests from client programs in the same or other computers. A given application in a computer may function as a client with requests for services from other programs and also as a server of requests from other programs.[134]

Single-Point Control: Helps reduce the total cost of application ownership by enabling applications and data to be deployed, managed and supported at the server. Single-point control enables application installations, updates and additions to be made once, on the server, which are then instantly available to users anywhere.

Smart Card: A credit-card-sized device with embedded microelectronics circuitry for storing information about an individual. This is not a key or token, as used in the remote access authentication process.

Spoofing: See IP Spoofing

State Full Evaluation: Methodology using mixture of proxy or filtering technology intermittently depending upon perceived threat [and/or need for "speed"].

Switch: A network device that selects a path or circuit for sending a unit of data to its next destination. A switch may also include the function of the router, a device or program that can determine the route and specifically what adjacent network point the data should be sent to. In general, a switch is a simpler and faster mechanism than a router, which requires knowledge about the network and how to determine the route.[135]

Symmetric Encryption: The encryption of data between two users using a single private key known to both parties.

Thin Client: A low-cost computing device that works in a server-centric computing model. Thin clients typically do not require state-of-the-art, powerful processors and large amounts of RAM and ROM because they access applications from a central server or network. Thin clients can operate in a Server-based Computing environment.

Token: A "token" is an authentication tool, a device utilized to send and receive challenges and responses during the user authentication process. Tokens may be small, hand-held hardware devices similar to pocket calculators or credit cards. See key.

Trojan Horse: 1) Any program designed to do things that the user of the program did not intend to do or that disguises its harmful intent. 2) Program that installs itself while the user is making an authorized entry; and, then are used to break-in and exploit the system.

Tunneling Router: A router or system capable of routing traffic by encrypting it and encapsulating it for transmission across an untrusted network, for eventual de-encapsulation and decryption. (See VPN)

Two-Factor Authentication: Two-factor authentication is based on something a user knows (factor one) plus something the user has (factor two). In order to access a network, the user must have both "factors" - just as he/she must have an ATM card and a Personal Identification Number (PIN) to retrieve money from a bank account, In order to be authenticated during the challenge/response process, users must have this specific (private) information.

User: Any person who interacts directly with a computer system.

User Identification: User identification is the process by which a user identifies himself to the system as a valid user. (As opposed to authentication, which is the process of establishing that the user is indeed that user and has a right to use the system.)
User Interface: The part of an application that the user works with. User interfaces can be text-driven, such as DOS, or graphical, such as Windows.

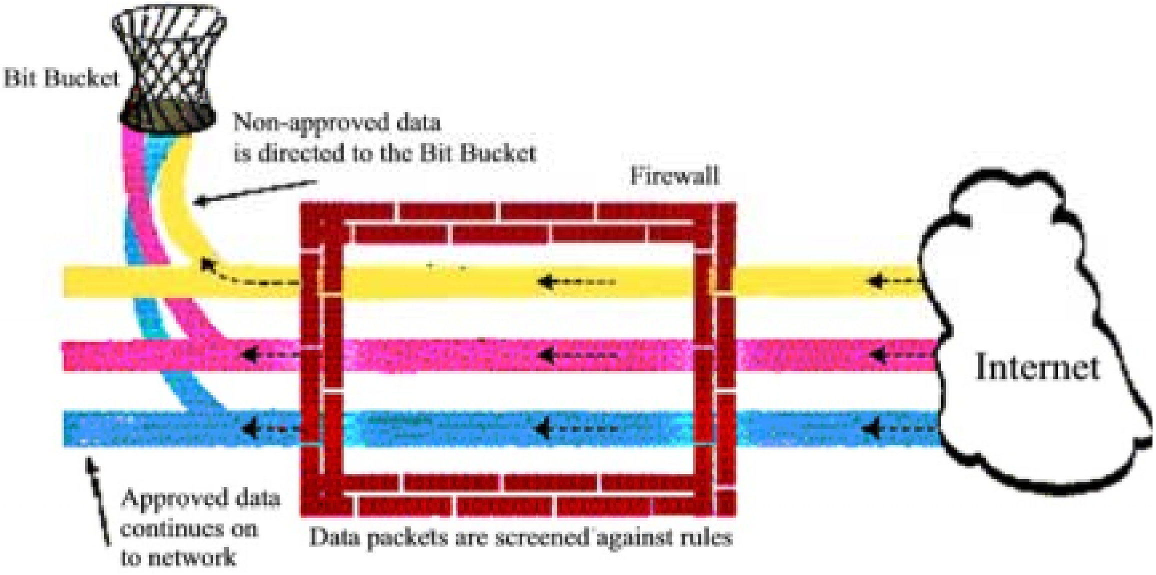
Virtual Private Network (VPN): A private data network that makes use of the public telecommunication infrastructure, maintaining privacy through the use of a tunneling protocol and security procedures. A virtual private network can be contrasted with a system of owned or leased lines that can only be used by one company. The idea of the VPN is to give the company the same capabilities at much lower cost by using the shared public infrastructure rather than a private one. Phone companies have provided secure shared resources for voice messages. A virtual private network makes it possible to have the same secure sharing of public resources for data. Companies today are looking at using a private virtual network for both extranets and wide-area intranets.[136]

Virus: A self-replicating code segment. Viruses may or may not contain attack programs or trapdoors.

Wide Area Network (WAN): A geographically dispersed telecommunications network. The term distinguishes a broader telecommunication structure from a local area network (LAN). A wide area network may be privately owned or rented, but the term usually connotes the inclusion of public (shared user) networks.[137]

Zoo virus: A virus which is rarely reported anywhere in the world, but which exists in the collections of researchers. A zoo virus has some "escaping" virus collections, and infecting user machines. Its prevalence could increase to the point that it was considered "in the wild".

Appendix C: Firewalls



Source: IDC and Solomon Smith Barney

Appendix D: Worldwide Firewall Software Revenue by Region and Operating Environment

Worldwide Firewall Software Revenue by Region and Operating Environment, 1999-2004E ($M)

	1999	2000E	2001E	2002E	2003E	2004E	1999 Share (%)	1999-2004E CAGR (%)	2004E Share (%)
Geographic region									
North America	299	338	386	435	475	532	55.7	12.2	45.0
Western Europe	137	176	217	232	264	284	25.5	15.7	24.0
Asia/Pacific	64	102	129	167	211	237	11.9	29.8	20.1
ROW	37	61	73	93	106	130	6.9	28.6	11.0
Total	537	677	805	926	1056	1182	100.0	17.1	100.0
Operating environment									
Mainframe	4	54	73	9	11	12	0.7	26.1	1.0
OS/400	0	0	0	0	0	0	0.0	NA	0.0
Unix	191	203	209	232	243	248	35.6	5.4	21.0
Linux/other open source	0	41	81	157	190	236	0.0	NA	20.0
Other host/server	90	54	32	28	21	24	16.8	-23.5	2.0
DOS/16-bit Windows	19	0	0	0	0	0	3.5	NA	0.0
Mac OS	0	7	8	9	11	12	0.0	159.6	1.0
32-bit Windows (including NT)	225	305	386	472	559	627	41.8	22.8	53.0
Platform independent	8	14	16	19	21	24	1.5	25.1	2.0
Embedded and subsystem	0	0	0	0	0	0	0.0	NA	0.0
Other single user	0	0	0	0	0	0	0.0	NA	0.0
Total	537	678	805	926	1056	1182	100.0	17.1	100.0

Source: IDC, 2000

Appendix E: Worldwide Firewall Software Revenue by Type

Worldwide Firewall Software Revenue by Type, 1999-2004E ($M)

	1999	2000E	2001E	2002E	2003E	2004E	1999 Share (%)	1999-2004E CAGR (%)	2004 Share (%)
Personal firewall	4	17	40	50	40	30	0.7	49.6	2.5
Distributed firewall	9	20	45	90	170	270	1.7	97.4	22.8
Enterprise	524	640	720	786	846	882	97.6	11.0	74.6
Total	537	677	805	926	1056	1182	100.0	17.1	100.0

Source: IDC, 2000

Appendix F: Worldwide Antiviral Software Revenue by Vendor Class

Worldwide Antiviral Software Revenue by Vendor Class, 1999-2004E ($M)

	1999	2000E	2001E	2002E	2003E	2004E	1999 Share (%)	1999-2004E CAGR (%)	2004E Share (%)
Vendor Class									
U.S. ISVs	961	1202	1430	1644	1842	2136	79.6	17.3	79.6
U.S. SVs	9	11	13	15	17	19	0.7	17.4	0.7
International ISVs	224	280	333	383	429	497	18.5	17.3	18.5
International SVs	14	18	21	25	28	32	1.2	17.3	1.2
Total									
United States	970	1213	1443	1659	1859	2155	80.3	17.3	80.3
International	238	298	354	408	457	529	19.7	17.3	19.7
Worldwide	1208	1511	1797	2067	2316	2684	100.0	17.3	100.0
Growth (%)		25.1	18.9	15.0	12.0	15.9			

Source: IDC, 2000

Appendix G: Worldwide Antiviral Software Revenue by Region and Operating Environment

Worldwide Antiviral Software Revenue by Region and Operating Environment, 1999-2004E ($M)

							1999	1999-2004E	2004E
	1999	2000E	2001E	2002E	2003E	2004E	Share (%)	CAGR (%)	Share (%)
Geographic region									
North America	669	815	970	1075	1180	1316	55.4	14.5	49.0
Western Europe	342	423	503	579	625	698	28.3	15.3	26.0
Asia/Pacific	137	181	216	289	347	456	11.4	27.1	17.0
ROW	59	91	108	124	162	215	4.9	29.3	8.0
Total	1207	1510	1797	2067	2314	2685	100	17.3	100
Operating environment									
Mainframe	0	0	0	0	0	0	0.0	NA	0.0
OS/400	0	0	0	0	0	0	0.0	NA	0.0
Unix	20	15	18	21	23	27	1.7	5.8	1.0
Linux/other open source	0	15	36	41	46	81	0.0	NA	3.0
Other host/server	293	347	395	434	463	510	24.2	11.7	19.0
DOS/16-bit Windows	279	332	323	289	231	161	23.1	-10.4	6.0
Mac OS	45	60	72	83	93	134	3.7	24.7	5.0
32-bit Windows (including NT)	572	740	952	1199	1458	1772	47.3	25.4	66.0
Platform independent	0	0	0	0	0	0	0.0	NA	0.0
Embedded and subsystem	0	0	0	0	0	0	0.0	NA	0.0
Other single user	0	0	0	0	0	0	0.0	NA	0.0
Total	1209	1509	1796	2067	2314	2685	100	17.3	100

Source: IDC, 2000

Appendix H: Worldwide Security 3A Software Revenue by Vendor Class and Vendor

Worldwide Security 3A Software Revenue by Vendor Class and Vendor, 1997-1999 ($M)

	1997	1998	1999	1999 Share (%)	1998-1999 Growth (%)
U.S. independent software vendors					
Computer Associates	208	386.6	502.2	23.9	29.9
Internet Security Systems	11.9	34.2	77.7	3.7	127.2
RSA Security	44.9	55	74.2	3.5	34.9
Entrust Technologies	18.7	40.9	72.4	3.5	77.1
AXENT Technologies	30.7	61	71.7	3.4	17.6
BindView	16	25.5	58	2.8	127.5
Mission Critical Software	11.3	14.8	26	1.2	76.3
Network Associates	64	22.6	21	1.0	-7.0
Utimaco Mergent	11	14	18.9	0.9	35.1
BMC Software	1.6	9.7	17	0.8	75.2
AOL	6.6	8.8	15.7	0.7	79.0
Cisco Systems	-	8	14	0.7	75.0
Sterling Software	17	14	14	0.7	0.0
Secure Computing	9.7	24	13.3	0.6	-44.7
V-One	-	9	12.1	0.6	34.0
GTE - CyberTrust Solutions	-	-	11.9	0.6	NA
Netegrity	-	2	9.9	0.5	395.0
Cybersafe	-	6	9.4	0.4	55.9
Rainbow Technologies	5	6.7	9	0.4	34.0
Aventail	-	6	8	0.4	34.0
Xcert	-	3	8	0.4	166.5
ODS	-	2.2	7.7	0.4	252.2
Websense	-	-	7	0.3	NA
enCommerce	-	-	6.8	0.3	NA
Cylink	3.5	4.6	6.5	0.3	41.4
Gradient Technologies	3.9	4.8	6.5	0.3	34.0
Symantec	9.8	1	6.4	0.3	540.0
Sterling Commerce	3.4	4.6	6	0.3	31.7
Candle	4	5.4	6	0.3	12.0
VeriSign	1	3.1	4.2	0.2	34.0
Novell	-	3	4	0.2	33.3
Tumbleweed Communication	-	-	3.8	0.2	NA
ValiCert	-	-	3	0.1	NA
Internet Dynamics	-	1.5	2	0.1	34.0
L3 Network Security	-	-	2	0.1	NA
Tripwire Security	-	-	2	0.1	NA
ClickNet Software	-	-	1.6	0.1	NA
Enlighten Software Solutions	-	-	1.2	0.1	170.3
New Era of Networks	0.7	0.8	1.1	0.1	34.0
Arcot Systems	-	-	1	<0.1	NA

Appendix H: Cont.

	1997	1998	1999	1999 Share (%)	1998-1999 Growth (%)
NetPro Computing	6.1	-	-	0.0	NA
SCH Technologies	0.5	0.6	-	0.0	-100.0
Veritas Software	0.5	-	-	0.0	NA
Subtotal U.S. ISVs	497.2	2781.4	1143.1	54.5	-58.9
Other U.S. ISVs	88	126.1	166	7.9	31.6
Total U.S. ISVs	585.2	2907.5	1309.1	62.4	-55.0
U.S. system vendors					
IBM	195.9	215.6	290	13.8	34.5
Hewlett-Packard	34.8	45	58.4	2.8	29.9
Sun Microsystems	21	28.5	40.4	1.9	41.8
Unisys	6	8.8	10.6	0.5	20.7
Subtotal U.S. SVs	257.7	297.9	399.4	19.0	34.1
Other U.S. SVs	25.9	42	48	2.3	14.3
Total U.S. SVs	283.6	339.9	447.4	21.3	31.6
International independent software vendors					
Content Technologies	7	11	22	1.0	100.0
Baltimore Technologies	-	15	20	1.0	33.3
Schumann AG	11.1	14	18.8	0.9	34.0
JSB	-	4	8	0.4	100.0
Trend Micro	-	-	7.9	0.4	NA
Elron Software	-	4	7.7	0.4	93.5
Beta Systems Software AG	3.7	3.7	3.8	0.2	1.8
Vasco	-	-	3.8	0.2	NA
Celo Communications	-	-	3	0.1	NA
Norman Data Defense	-	3	1	<0.1	-66.7
Macro 4	-	-	-	0.0	14.9
Systar SA	0.8	1.1	-	0.0	-100.0
Subtotal international ISVs	22.7	56	96.2	4.6	71.8
Other international ISVs	16.3	84	129.3	6.2	53.9
Total international ISVs	39	140	225.5	10.7	61.1
International system vendors					
Groupe Bull	26.8	26.6	35	1.7	31.3
Fujitsu	22.5	23.9	23.4	1.1	-2.0
Hitachi	15.5	15.3	21.1	1.0	38.0
NEC	-	2	5	0.2	150.0
Subtotal international SVs	64.8	67.8	84.5	4.0	24.6
Other international SVs	24.9	28	32	1.5	14.3
Total international SVs	89.7	95.8	116.5	5.6	21.6
Total United States	868.8	1249.7	1756.5	83.7	40.6
Total international	128.8	235.8	342	16.3	45.0
Total worldwide	997.6	1485.5	2098.5	100.0	41.3

Source: IDC, 2000

Appendix I: Worldwide 3A Software Revenue by Region and Operating Environment

Worldwide 3A Software Revenue by Region and Operating Environment, 1999-2004E ($M)

	1999	2000E	2001E	2002E	2003E	2004E	1999 Share (%)	1999-2004E CAGR (%)	2004E Share (%)
Geographic region									
North America	1219.1	1600.6	2004.5	2489.9	3124.3	3930.8	58.1	26.4	55.0
Western Europe	556.3	748.0	964.1	1228.2	1553.7	1951.1	26.5	28.5	27.3
Asia/Pacific	221.4	304.3	395.2	511.4	661.0	857.6	10.6	31.1	12.0
ROW	101.7	138.1	180.7	236.7	310.7	407.3	4.9	32.0	5.7
Total	2098.5	2791.0	3544.6	4466.2	5649.7	7146.9	100.0	27.8	100.0
Operating environment									
Mainframe	450.8	558.2	638.0	759.3	904.0	1072.0	21.5	18.9	15.0
OS/400	11.3	14.0	16.0	20.1	22.6	28.6	0.5	20.4	0.4
Unix	759.1	879.2	1051.0	1208.1	1463.3	1686.7	36.2	17.3	23.6
Linux/other open source	1.0	139.6	283.6	535.9	847.5	1357.9	0.0	323.2	19.0
Other host/server	197.2	251.2	304.8	366.2	423.7	500.3	9.4	20.5	7.0
DOS/16-bit Windows	77.6	94.9	106.3	111.7	113.0	107.2	3.7	6.7	1.5
Mac OS	1.1	0.0	0.0	0.0	0.0	0.0	0.1	NA	0.0
32-bit Windows (including NT)	577.5	809.4	1059.8	1339.9	1694.9	2144.1	27.5	30.0	30.0
Platform independent	20.8	27.9	42.5	58.1	79.1	107.2	1.0	38.8	1.5
Embedded and subsystem	0.0	16.7	42.5	67.0	101.7	142.9	0.0	NA	2.0
Other single user	2.0	0.0	0.0	0.0	0.0	0.0	0.1	NA	0.0
Total	2098.5	2791.0	3544.6	4466.2	5649.7	7146.9	100.0	17.1	100.0

Source: IDC, 2000

Appendix J: Worldwide Security 3A Software Revenue by Vendor Class and Operating Environment

Worldwide Security 3A Software Revenue by Vendor Class and Operating Environment, 1999 ($M)

	Mainframe	OS/400	Unix	Linux/Other Open Source	Other Host/Server	DOS/16-bit Windows	Mac OS	32-Bit Windows (Including NT)	Platform Independent	Embedded Subsystem	Other Single User
Vendor Class											
U.S. ISVs	223	8	460	1	134	56	1	404	20	0	2
U.S. SVs	142	3	206	0	10	19	0	67	0	0	0
International ISVs	30	0	59	0	42	3	0	91	1	0	0
International SVs	56	0	34	0	11	0	0	16	0	0	0
Total											
United States	365	11	666	1	144	75	1	471	20	0	2
International	86	0	93	0	53	3	0	106	1	0	0
Worldwide	451	11	759	1	197	78	1	578	21	0	2
Share (%)	21.5	0.5	36.2	0.0	9.4	3.7	0.1	27.5	1.0	0.0	0.1

Source: IDC, 2000

Appendix K: The Number of Possible Keys Combinations

The Number of Possible Keys Combinations					
Number of Possible Keys	**Number of Bits in a Cryptographic Key**				
	1	**2**	**3**	**4**	**5**
1	0	00	000	0000	00000
2	1	01	001	0001	00001
3		10	010	0010	00010
4		11	011	0011	00011
5			100	0100	00100
6			101	0101	00101
7			110	0110	00110
8			111	0111	00111
9				1000	01000
• • •				• • •	• • •
16				1111	01111
• • •				• • •	• • •
32					11111
Source: Hambrecht & Quist					

Appendix L: World Encryption Software Revenue by Vendor

Worldwide Encryption Software Revenue by Vendor (Alphabetical Listing), 1997-1999 ($M)

				1999	1998-1999
	1997	1998	1999	Share (%)	Growth (%)
U.S. independent software vendors					
RSA Security	27	39	51.2	38.3	31.3
Network Associates	7.4	8.6	7	5.2	-19.1
Certicom	0.8	1.5	6.5	4.9	333.2
Symantec	1	2	5	3.7	150.1
AXENT Technologies	1.3	2.6	3.1	2.3	19.2
RPK	-	-	1	0.7	900.0
NovaStor	-	0.6	0.6	0.4	0.0
Cylink	1.5	-	-	0.0	NA
Globetrotter Software	1	-	-	0.0	NA
Subtotal U.S. ISVs	40	54.5	74.4	55.6	36.7
Other U.S. ISVs	7.8	5.2	6.7	5.0	28.8
Total U.S. ISVs	47.8	59.7	81.1	60.6	36.0
U.S. system vendors					
IBM	1.6	2.6	3	2.2	16.0
Subtotal U.S. SVs	1.6	2.6	3	2.2	16.0
Other U.S. SVs	0.6	1	1.3	1.0	30.0
Total U.S. SVs	2.2	3.6	4.3	3.2	19.9
International independent software vendors					
F-Secure	7	10	12.5	9.4	25.2
Baltimore Technologies	-	3	4	3.0	33.3
Subtotal international ISVs	7	13	16.5	12.3	27.1
Other international ISVs	8	9.5	12.2	9.1	28.4
Total international ISVs	15	22.5	28.7	21.5	27.6
International system vendors					
Hitachi	-	7.6	11.4	8.5	49.6
Fujitsu	3.3	3.5	3.3	2.5	-3.4
Subtotal international SVs	3.3	11.1	14.8	11.0	33.1
Other international SVs	2.9	3.9	5	3.7	28.2
Total international SVs	6.2	15	19.8	14.8	31.8
Total United States	50	63.3	85.4	63.8	34.9
Total international	21.2	37.5	48.5	36.2	29.3
Total worldwide	71.2	100.8	133.9	100.0	32.8

Source: IDC, 2000

Appendix M: Worldwide Encryption Software Revenue by Region and Operating Environment

Worldwide Encryption Software Revenue by Region and Operating Environment, 1999-2004E ($M)

	1999	2000E	2001E	2002E	2003E	2004E	1999 Share (%)	1999-2004E CAGR (%)	2004E Share (%)
Geographic region									
North America	71	89	102	111	116	120	52.8	11.1	50.5
Western Europe	35	45	54	61	67	72	25.8	15.9	30.5
Asia/Pacific	22	27	31	33	34	34	16.5	9.4	14.5
ROW	7	8	10	10	11	11	4.9	9.9	4.5
Total	134	169	196	215	228	237	100.0	12.1	100.0
Operating environment									
Mainframe	15	17	20	22	23	24	10.8	10.3	10.0
OS/400	0	0	0	0	0	0	0.0	NA	0.0
Unix	54	61	58	55	43	32	40.4	-10.0	13.4
Linux/other open source	0	7	12	17	23	33	0.0	NA	14.0
Other host/server	8	8	9	9	8	7	6.0	-2.1	3.0
DOS/16-bit Windows	7	7	7	4	2	0	5.2	NA	0.0
Mac OS	3	3	3	3	3	4	2.2	3.7	1.5
32-bit Windows (including NT)	40	54	67	75	87	93	29.9	18.3	39.0
Platform independent	1	1	2	2	2	3	0.6	26.6	1.1
Embedded and subsystem	7	10	20	28	37	43	5.0	44.8	18.0
Other single user	0	0	0	0	0	0	0.0	NA	0.0
Total	134	169	196	215	228	237	100.1	17.1	100.0

Source: IDC, 2000

Appendix N: Worldwide Encryption Software Revenue by Vendor Class and Operating Environment

Worldwide Encryption Software Revenue by Vendor Class and Operating Environment, 1999 ($M)

				Linux/Other	Other	DOS/16-Bit		32-Bit Windows	Platform	Embedded	Other Single
	Mainframe	OS/400	Unix	Open Source	Host/Server	Windows	Mac OS	(including NT)	Independent	/Subsystem	User
Vendor Class											
U.S. ISVs	0	0	45	0	4	5	2	20	1	5	0
U.S. SVs	3	0	1	0	0	0	0	0	0	0	0
International ISVs	0	0	5	0	4	2	1	15	0	1	0
International SVs	12	0	3	0	0	0	0	5	0	0	0
Total											
United States	3	0	46	0	4	5	2	20	1	5	0
International	12	0	8	0	4	2	1	20	0	1	0
Worldwide	15	0	54	0	8	7	3	40	1	7	0
Share (%)	11	0.0	40.0	0.0	6.0	5.0	2	30	1	5	0

Source: IDC, 2000

Appendix O: Worldwide Encryption Software Revenue by Vendor Class

Worldwide Encryption Software Revenue by Vendor Class, 1999-2004E ($M)

	1999	2000E	2001E	2002E	2003E	2004E	1999 Share (%)	1999-2004E CAGR (%)	2004E Share (%)
Vendor Class									
U.S. ISVs	81	102	119	130	138	144	60.6	12.1	60.6
U.S. SVs	4	5	6	7	7	8	3.2	12.1	3.2
International ISVs	29	36	42	46	49	51	21.4	12.1	21.4
International SVs	20	25	29	32	34	35	14.8	12.1	14.8
Total									
United States	85	108	125	137	146	151	63.8	12.1	63.8
International	49	61	71	78	83	86	36.2	12.1	36.2
Worldwide	134	169	196	215	228	237	100.0	12.1	100.0
Growth (%)		26	16	10	6	4			

Source: IDC, 2000

Appendix P: Worldwide Encryption Software Revenue by Segment

Worldwide Encryption Software Revenue by Segment, 1999-2004E ($M)

	1999	2000E	2001E	2002E	2003E	2004E	1999 Share (%)	1999-2004E CAGR (%)	2004E Share (%)
Encryption algorithm and developer tools	86.3	107.2	124.4	138.3	149.7	155.6	64.5	12.5	65.6
File encryption applications	47.4	61.4	71.2	76.9	78.3	81.6	35.5	11.5	34.4
Total	133.7	168.6	195.6	215.2	228	237.2	100	12.1	100

Source IDC,2000

Endnotes:

[1] Congressional Statement Federal Bureau of Investigation. 2001. “Statement for the Record of Thomas T. Kubic, Deputy Assistant Director Federal Bureau of Investigation.” At <http://www.fbi.gov/congress/congress01/kubic052301.htm>. August 2001.
[2] *Ibid.*
[3] McDonald, Tim. 2000. E-Commerce Times. “Report: Year's Hack Attacks To Cost $1.6 Trillion.” At <http://www.ecommercetimes.com/perl/story/3741.html>. August 2001.
[4] Jones, Chuck. 2001. “Internet Security Software: The Ultimate Internet Infrastructure - Part 2.” At <http://www.itaudit.org/forum/internet/f405in.htm>. August 2001.
[5] Cunningham, Cara. 2001. Red Herring. “Digital Security Defies Slowdown.” At <http://www.redherring.com/index.asp?layout=special_report_gen&channel=10000001&doc_id=330019833&rh_special_report_id=710000071>. August 2001.
[6] http://www.distributedfirewalls.com/firewall.html. August 2001.
[7] http://www.checkpoint.com. August 2001.
[8] http://enterprise.cnet.com/enterprise/0-9567-7-2481745.html. August 2001.
[9] http://www.prnewswire.com/cgi-bin/stories.pl?ACCT=105&STORY=/www/story/04-18-2001/0001471701. August 2001.
[10] http://www.nwfusion.com/news/2001/0214isa.html. August 2001.
[11] Felker, Nicole. IDC. Interviewed by Craig Bingham. August 14, 2001.
[12] http://www.cisco.com. August 2001.
[13] Kolodgy, Charles. IDC. Interviewed by Craig Bingham. August 2, 2001.
[14] http://www.telecominvestormag.com/telecom/newstrends/headlinesdetail.jhtml?headlineID=1519
[15]http://www.technologyevaluation.com/research/researchhighlights/security/1999/11/news_analysis/NA_ST_LPT_11_10_99_12.asp. August 2001.
[16] http://www.robertel.com/frame3.htm. August 2001.
[17] http://news.cnet.com/investor/news/newsitem/0-9900-1028-6377587-0.html. August 2001.
[18] http://lapserver.itc.gu.edu.au/gartner/research/ras/94200/94248/94248.html. August 2001.
[19] http://www.telecominvestormag.com/telecom/newstrends/headlinesdetail.jhtml?headlineID=1519
[20] Ibid.
[21] http://www.advisor.com/Articles.nsf/aidp/OLSEE079. August 2001.
[22] http://www.itaudit.org/forum/internet/f411in.htm. August 2001.
[23] Ibid.
[24] Ibid.
[25] http:// www.nortelnetworks.com/products/01/vpn. August 2001.
[26] http://www.nwfusion.com/news/2000/0308vpnsoft.html. August 2001.
[27] http://www.nwfusion.com/edge/news/2000/112377_11-20-2000.html. August 2001.
[28] http://www.nwfusion.com/net.worker/news/2000/1201intel.html. August 2001.
[29] http://techguide.zdnet.com/html/intsec_print/index.shtml. August 2001.
[30] http://www.brightmail.com. August 2001.
[31] http://www.checkpoint.com/press/partners/1997/axent0497.html. August 2001.
[32] http://www.trendmicro.com.hk/full_doc29.htm. August 2001.
[33] http://www.sophos.com. August 2001.
[34] http://www.zdnet.com/zdhelp/stories/main/0,5594,2571084,00.html. August 2001.
[35] http://www.itaudit.org/forum/internet/f415in.htm. August 2001.
[36] Ibid.
[37] http://victoria.tc.ca/int-grps/books/techrev/avrevfaq.html. August 2001.
[38] http://www.bankofamerica.com.hk/english/onlinebank/signin/glossary.html. August 2001.
[39] http://members.aol.com/Winchel3/Links/Legal/Signatures/SignaturesLegalLinks.htm. August 2001.
[40] http://www.itaudit.org/forum/internet/f414in.htm. August 2001.
[41] http://www-4.ibm.com/software/security/registry/library/whitepapers/crypto.html. August 2001.
[42] http://www.tda.ecrc.ctc.com/kbase/doc/brief/digsig.htm. August 2001.
[43] http://www.itsecurity.com/tecsnews/feb2001/feb413.htm. August 2001.
[44] http://www.law.upenn.edu/bll/ulc/fnact99/1990s/ueta99.htm. August 2001.
[45] http://www.rsa.com/solutions/vpn/framework.html. August 2001.

[46] http://www.networkcomputing.com/1006/1006f1.html. August 2001.
[47] http://www.usenix.org/publications/library/proceedings/lisa98/full_papers/grubb/grubb_html/grubb.html. August 2001.
[48] http://www.itaudit.org/forum/internet/f403in.htm. August 2001.
[49] http://www.whatis.com/definition/0,289893,sid9_gci212062,00.html. August 2001.
[50] Ibid.
[51] http://members.aol.com/Winchel3/Links/Legal/Signatures/SignaturesLegalLinks.htm. August 2001.
[52] http://csrc.nist.gov/encryption/aes/draftfips/fr-AES-200102.html. August 2001.
[53] http://csrc.nist.gov/encryption/aes/aesfact.html. August 2001.
[54] http://www.hipaadvisory.com/regs/securityandelectronicsign/electronicsignature.htm
[55] http://www.remotefirewalls.com/hipaa.htm
[56] http://www.checkpoint.com/press/2000/idc112800.html, July 19, 2001.
[57] Ibid.
[58] http://profiles.wisi.com/profiles/scripts/corpinfo.asp?cusip=C376I7320, July 25, 2001.
[59] http://www.checkpoint.com/press/2000/ua062600.html, July 25, 2001.
[60] http://profiles.wisi.com/profiles/scripts/corpinfo.asp?cusip=749719100, July 20, 2001.
[61] http://profiles.wisi.com/profiles/scripts/corpinfo.asp?cusip=871503108, July 20, 2001.
[62] http://profiles.wisi.com/profiles/scripts/corpinfo.asp?cusip=89486M206, July 20, 2001.
[63] http://bvlive01.iss.net/issEn/delivery/prdetail.jsp?fid=110199187.plt, July 20, 2001.
[64] http://www.hoovers.com, Hoovers Subscriber Page, July 19, 2001.
[65] Burke, Brian and Christian Christiansen and Nora Freedman, IDC, April 2000.
[66] http://www.itworld.com/App/650/CWSTO57807/pfindex.html, July 27, 2001.
[67] http://www.microsoft.com/technet/treeview/default.asp?url=/TechNet/prodtechnol/isa/evaluate/isatecov.asp, August 2, 2001.
[68] http://newsroom.cisco.com/dlls/corpfact.html, August 2, 2001.
[69] http://www.cisco.com/univercd/cc/td/doc/pcat/fw.htm, August 2, 2001.
[70] http://www.nokia.com/vpn, August 6, 2001.
[71] http://www.netscreen.com/aboutus/articles/news070201b.html, July 31, 2001.
[72] http://www.netscreen.com/aboutus/index.html, August 6, 2001.
[73] http://www.palmchip.com/about_palmchip.html, August 8, 2001.
[74] http://www.questlink.com/QL/CDA/Research/CompanyProfile/0,1756,0_73550_0,00.html, August 8, 2001.
[75] http://www.rainbow.com/about.html, July 26, 2001.
[76] http://www.SonicWALL.com/corporate_info/, August 2, 2001.
[77] http://www.watchguard.com/about/, July 27, 2001.
[78] http://www.authentica.com/company/index.html, July 26, 2001.
[79] http://www.netegrity.com/AboutUs/index.cfm, July 26, 2001.
[80] http://www.network-1.com/products/index.html, August 8, 2001.
[81] http://www.systemsoft.com/l-2/about.htm, July 26, 2001.
[82] http://www.hoovers.com, Hoovers Subscriber Page, July 19, 2001.
[83] http://www.hoovers.com/co/capsule/8/0,2163,54478,00.html, July 23, 2001.
[84] http://www.iplanet.com/solutions/customer_profile/hitachi_america_1_3j.html, July 31, 2001.
[85] http://www.hoovers.com/co/capsule/0/0,2163,59820,00.html, July 23, 2001.
[86] http://www.counterpane.com/background.html, July 26, 2001.
[87] http://www.cylink.com/corporate/corppage.htm, July 26, 2001.
[88] http://www.litronic.com/company/company_info.html, July 26, 2001.
[89] http://www.rainfinity.com/rainfinity/rainfinity.shtml, July 26, 2001.
[90] http://www.redcreek.com/index.htm, July 26, 2001.
[91] http://www.redcreek.com/about/index.html, July 26, 2001.
[92] http://www.perfectotech.com/news/releases/jul01/press07-2301a.html, August 6, 2001.
[93] http://www.securecomputing.com/index.cfm?sKey=1, July 26, 2001.
[94] http://www.securify.com/company/index.html, July 26, 2001.
[95] http://corporate.verisign.com/about/index.html, July 26, 2001.
[96] http://www.hoovers.com/co/capsule/4/0,2163,56244,00.html, July 23, 2001.

[97] http://www.bindview.com/about/, July 27, 2001.
[98] http://www.infraworks.com/company.html, August 8, 2001.
[99] http://www.pentasafe.com/ourculture/, August 8, 2001.
[100] http://www.aventail.com/about/default.asp, July 27, 2001.
[101] http://www.cybersafe.com/company/corporateprofile.html, July 27, 2001.
[102] http://profiles.wisi.com/profiles/scripts/corpinfo.asp?cusip=204912109, July 27, 2001.
[103] http://www.ibm.com/services/e-business/netspec.html, July 27, 2001.
[104] http://profiles.wisi.com/profiles/scripts/corpinfo.asp?cusip=459200101, July 20, 2001
[105] Vincent, Winchel Todd, III. 1997. "Digital and Electronic Signatures." At <http://members.aol.com/Winchel3/Links/Legal/Signatures/SignaturesLegalLinks.htm>. July 2001.
[106] National Center for Education Statistics. 1998. "State Comparison of Education Statistics: 1967-1996-1997." At <http://nces.ed.gov/pubs98/98018.pdf>. August 2001.
[107] Facelli, Julio, School of Computing University of Utah. Interviewed by Derek Englis, Chris Pressler, and Craig Bingham. July 23, 2001.
[108] "Digital Signature Legislation." http://home.earthlink.net/~hldettling/summary.htm
[109] Lash, Alex. 1997. "Utah Grants First Certificate Authority." CINET. At < http://news.cnet.com/news/0-1005-200-324556.html?tag=rltdnws>. August 2001.
[110] "Utah Governor Signs Digital State Legislation." At < http://www.fedsources.com/spotlight/archive/state/s032999-5.asp>. July 2001.
[111] http://www.developmentalliance.com/legclimates/UT.htm
[112] At<http://www.accessdata.com>. August 2001.
[113] "Arcanvs Corporate Profile." 2000. At < http://www.arcanvs.com/info/corporate_profile.html>. July 2001.
[114] "Digital Signature Trust Company Overview." 2001. At <http://www.digsigtrust.com/company/index.html>. July 200l.
[115] Earth Speak International. At <http://www.earthspeakinternational.com/>. July 2001.
[116] iLumin: About the Company. At <http://www.ilumin.com/company/company_overview.asp>. July 2001.
[117] Novell Security Services. At <http://www.novell.com/products/index.html#SecurityServices>. July 2001.
[118] <http://www.usertrust.com/>. July 2001.
[119] http://searchsolaris.techtarget.com/sDefinition/0,,sid12_gci344759,00.html. August 2001.
[120] http://searchvb.techtarget.com/sDefinition/0,,sid8_gci211545,00.html. August 2001.
[121] http://whatis.techtarget.com/definition/0,289893,sid9_gci213831,00.html. August 2001.
[122] http://science.kennesaw.edu/~mcmurray/csis3600dfd.html. August 2001.
[123] http://www.dmreview.com/master.cfm?NavID=32&KeywordID=D. August 2001.
[124] http://whatis.techtarget.com/definition/0,289893,sid9_gci211947,00.html. August 2001.
[125] http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci211953,00.html. August 2001.
[126] http://searchwin2000.techtarget.com/sDefinition/0,,sid1_gci212065,00.html. August 2001.
[127] http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci212089,00.html. August 2001.
[128] http://searchnetworking.techtarget.com/sDefinition/0,,sid7_gci212176,00.html. August 2001.
[129] http://searchwebmanagement.techtarget.com/sDefinition/0,,sid27_gci212254,00.html. August 2001.
[130] http://searchwebmanagement.techtarget.com/sDefinition/0,,sid27_gci212377,00.html. August 2001.
[131] http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci214299,00.html. August 2001.
[132] http://www.whatis.com/definition/0,289893,sid9_gci214245,00.html. August 2001.
[133] http://searchnetworking.techtarget.com/sDefinition/0,,sid7_gci212924,00.html. August 2001.
[134] http://searchenterpriseservers.techtarget.com/sDefinition/0,,sid25_gci212964,00.html. August 2001.
[135] http://searchnetworking.techtarget.com/sDefinition/0,,sid7_gci213079,00.html. August 2001.
[136] http://searchnetworking.techtarget.com/sDefinition/0,,sid7_gci213324,00.html. August 2001.
[137] http://searchnetworking.techtarget.com/sDefinition/0,,sid7_gci214117,00.html. August 2001.